A CONCEPTUAL FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

Student	**Dr. P.C. Duvenage**
Student number	**908202368**
Study Leader	**Prof. S.H. von Solms**
Programme	**D.Com (Computer Science)**
Faculty	**Faculty of Science** **Academy of Computer Science and Software Engineering**
Date	**13 September 2019**

A CONCEPTUAL FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

by

Petrus Carolus Duvenage

Thesis

submitted in partial fulfilment of the requirements for the degree

Doctor of Commerce

in

Computer Science

in the

Faculty of Science

at the

University of Johannesburg

Supervisor: Prof. S.H. von Solms

September 2019

ABSTRACT

Despite the sharp increase in global spend on cybersecurity during this decade, the extent and impact of serious cyber breaches are escalating. This can, in part, be ascribed to current approaches not proactively engaging morphing threats. It is clear that conventional, defensive cybersecurity solutions alone no longer offer adequate protection against threats posed by actors such as nation states, crime syndicates, corporate spies, terrorists, hacktivists and rogue individuals. There is growing acceptance that a multidisciplinary approach, which coherently combines offensive and defensive thrusts, is required to effectively secure cyber assets. For state and non-state actors with sizable cyber interests, cyber counterintelligence (CCI) offers such a practicable approach. Concurrent with the growing interest in CCI in corporate boardrooms and the corridors of governments, CCI is emerging as a field of academic enquiry.

Both the effective practice and academic progression of CCI depend on sound theory. Yet, in the consulted literature, purposeful attempts to advance a theory for CCI are limited and fragmented. More specifically, and considering CCI's incipient academic status, there is a need for an overarching conceptual framework for CCI (FCCI). In addition to guiding practice, such a framework can be a baseline for further multidisciplinary academic enquiry.

The aim of this thesis is to advance such a conceptual framework. The framework consists of eight notional building blocks essential to an academically credible and practically useful FCCI. In line with CCI's multidisciplinary nature, the FCCI's design draws on various academic fields.

However, the FCCI and its building blocks cannot be explicated in detail within the confines of a thesis. Only the essential contours of, and rationale behind, the FCCI's design are therefore provided. The FCCI is qualified as an exploratory postulation, hopefully constructive to practice and academic discourse.

ACKNOWLEDGMENTS

This thesis is, above all, in memory of my late father and mother. The ethos of inquisitiveness and compassionate respect in which we were raised, as well as their personal sacrifices, afforded us (their children and grandchildren) immeasurable opportunities.

I also express my appreciation to the following:

- My sons (Werner and Francois) and the rest of the Duvenage clan - this thesis is dedicated to you.
- Reana, for her encouragement and support.
- In what is decidedly more than a customary remark, my study leader, Professor Basie von Solms for his mentorship and guidance. It was indeed a privilege to conduct the study under the guidance of an academic of his stature.
- Yulna, Sarie, Marley, Riaan, Pauleen, Ida, Wandi, Hermien, Karien, Paula, Merlin, Kobie, Ntoagae, Herma and Christine for their interest and respective contributions.
- My 'comrades in arms', Dr Victor Jaquire and Thenjiwe Sithole – I salute you.
- My employer, the State Security Agency, for supporting the study. The relevant members of the executive management will be thanked in person for what, career-wise, was simultaneously a most empowering and humbling experience.
- Piet Ferreira, a 'professor of life', for his wisdom and perspectives.
- My friends, several of whom are also colleagues, for their interest.
- To my present and former colleagues: *Ars contra artem*.

NOTES ON THE WRITING STYLE AND APPROACH

For ease of reading, the pronouns 'we, 'us' and 'our' are used in this thesis. The intended meaning of these pronouns is determined by the context in which they are used. In addition to this less formalistic writing, chapters, sections and subsections are frequently summarised. While this in some instances results in repetition, it is hoped that these summaries will add to an overall easier reading experience.

For the same reason, each chapter is a ‘standalone unit’ which can be read without the reader having to excessively page backward and forward to previous and subsequent chapters. Consequently, there are overlaps between chapters and, where needed for context, recapitulations of key contentions made elsewhere in the thesis.

NOTES ON THE AUTHOR’S EXPERIENCE

The author’s career within statutory military and intelligence structures spans three decades. He served as an officer in the South African Defence Force, the National Intelligence Service, the National Intelligence Agency and the State Security Agency. For most of his career, he specialised in counterintelligence and he has extensive expertise in various aspects of this field. He has a PhD from the University of Pretoria and has been holding a Senior Research Fellowship at the Academy for Computer Science and Software Engineering (University of Johannesburg) for the past four years.

Without negating the academic imperatives posed to a doctoral thesis, some assertions and contentions in this thesis are based on the author’s experience.

TABLE OF CONTENTS

LIST OF FIGURES

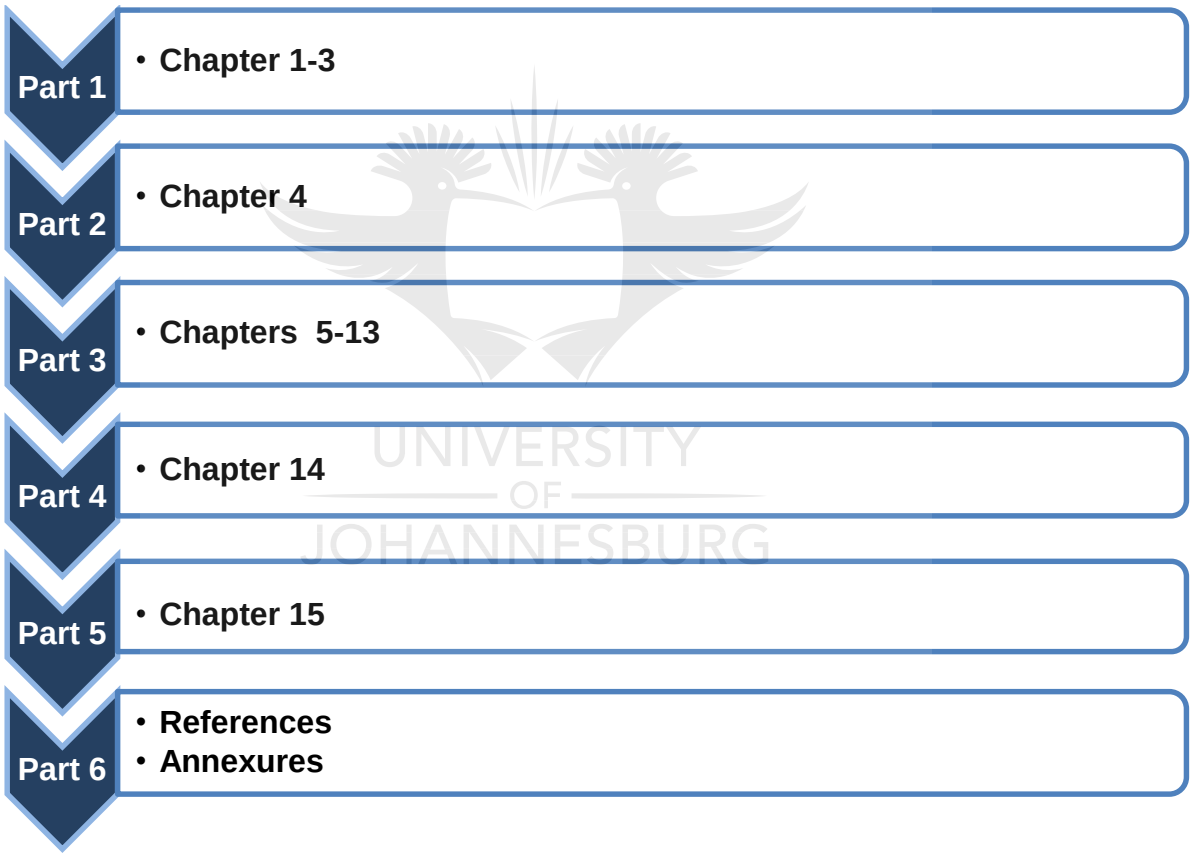
LIST OF TABLES

LIST OF ABBREVIATIONS

Artificial Intelligence ..... AI
Awareness, education and training ..... AET
Awareness and training programme ..... ATP
Communication intelligence ..... COMINT
Communication security ..... COMSEC
Counterintelligence CI
Cyber counterintelligence CCI
Cyberintelligence ..... CYBINT
Dynamic measurement photograph ..... DMPINT
Electronic intelligence ..... ELINT
Electronic, optical intelligence ..... ELECTRO-OPINT
[Conceptual] framework for cyber counterintelligence ..... FCCI
Human Intelligence ..... HUMINT
Information and technological systems security ..... INSYSEC
Information security ..... INFOSEC
Technical security countermeasures ..... TSCMs
Infrared intelligence ..... IRINT

Imagery Intelligence ..... IMINIT
Laser intelligence ..... LASINT
Measurement and signature intelligence ..... MASINT
Satellite Intelligence ..... SATINT
Social Media Intelligence .....SOCMINT
Telemetry intelligence ..... TELINT

This thesis consists of the following six parts:



PART 1

FOUNDATION AND CONFIGURATION OF THE CONCEPTUAL FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

Part 1 starts with outlining the academic and practical need for a conceptual framework for cyber counterintelligence (FCCI). This is followed by the stating of the research problem, research questions and hypothesis. We then advance the essential features of a conceptual framework to which our FCCI should comply. To inform the FCCI's design, an evaluative literature study is also conducted. Part 1 consists of the following chapters:

- Chapter 1: Introduction
- Chapter 2: Features and Configuration of the Conceptual Framework for Cyber Counterintelligence
- Chapter 3: Evaluative Literature Study

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION AND BACKGROUND

Despite a sharp increase in global spend on cybersecurity during this decade, the extent and impact of serious cyber breaches are escalating. This can, in part, be ascribed to current approaches not proactively engaging morphing threats. Several of the most serious breaches are the result of, or can at the very least be closely linked to, actors (governments, criminal syndicates, business entities) utilising the cyberspace as a primary conduit for executing intelligence and counterintelligence operations (Prunckun 2018; Stech & Heckman 2018; Buchanan 2016; Duvenage, Jaquire & von Solms 2018a). Some quotes attesting to this escalating trend are:

- "Nonstate entities, including international terrorist groups and transnational organized crime organizations, will continue to employ and potentially improve their intelligence capabilities, which include human, cyber, and technical means. Like state intelligence services, these non-state entities recruit human sources and conduct physical and technical surveillance to facilitate their activities and avoid detection and capture." – Director of National Intelligence, United States of America (US) (Coats 2018)
- "The primary motivation behind global cyber activity has now shifted from disparate activities carried out by individuals, groups and criminal gangs pursuing short-term financial gain to skilled adversaries driven by broader agendas." (Crowdstrike 2016)
- "[D]istinguishing criminal gangs from nation-state actors [is] a challenge…Tools and tradecraft become harder to tell apart…some financial threat groups that we track exhibit traits that look more like state-sponsored APT activity." (Mandiant – FireEye 2015)

The signature role of counterintelligence (CI) and its subset cyber counterintelligence (CCI) is precisely the pro-active anticipation, detection, analysis, engagement, exploitation and neutralisation of such threats. Properly conceptualised and implemented as part of CI, CCI is a practicable approach for governments, businesses and other sizable entities. The demand for, and on, CCI is sure to increase. Of late,

CCI's growing significance in especially larger companies is increasingly clear (Panda Security Labs 2018).

Effective CCI practice presupposes a sound theoretical foundation. Theoretical constructs are not 'nice to have' academic 'toys'. Theoretical constructs, such as frameworks and models, condition our thinking and our approach to practice. Poor theory leads to poor practice. Consequently, within intelligence and CI the price for poor theory is ultimately paid in costly failures and damaging breaches.

Herein also lays the glitch. As an academic field and formalised area of academic research, CCI is in its infancy and even the agenda for its development has in various respects not been set. One of the priority items on this agenda ought to be an overarching conceptual framework which (albeit tentatively) defines, describes and relates key constructs (building blocks). In this regard, Krishnan (2009) righty asserts that an academic discipline "should have theories and concepts that can organise accumulated specialist knowledge effectively".

CCI's under-theorised status stands in sharp contrast to the rich and expansive body of literature focused on the closely related field of information warfare and its subset cyber warfare. A few examples of such works – spanning more than two decades – include those by Molander, Riddle & Wilson (1996), Denning (1999), Kopp (2000), Hutchinson & Warren (2001), Jones, Kovacich & Luzwick (2002), Hutchinson (2006), Armistead (2004), Clarke & Knake (2010), Armistead (2010), van Niekerk & Maharaj (2011), Warren (2013), Andress & Winterfeld (2014), Janczewski & Caelli (2016) and Buchanan (2016).

The theoretical paucity on CCI should be viewed within the context of the persisting theoretical poverty of CI in general. As a pillar of state security, CI has been practised and described for millennia. Some enduring CI principles were, for example, recorded in 500 B.C. by the much-quoted Sun Tzu in a subsection devoted to the use of spies and counterspies (Duvenage & von Soms 2015, Giles 2002). This said, there is surprisingly few works in the public domain which explain multidisciplinary CI's theory and practice – be it within government or in the corporate world (Prunckun 2012, 2014). Consequently – and even within well-resourced, developed countries such as the US – "CI remains little known or understood among scholars or practitioners of national security and policymaking" (Van Cleave 2007). The few works which explain multidisciplinary CI theory and practice (e.g. Prunckun 2012, 2014; Duvenage 2011) do not venture into any detail on CCI.

CCI is, of course, a much more recent branch of CI. CCI existed *de facto* in the state security apparatus of countries such as the US "since the introduction of IT to intelligence, defence and national security" (*cf.* French & Kim 2009, Stone & Tucker 1988). It was, however, only in the late 1990s that CCI crystallised as a formalised CI field within the state apparatus (French & Kim 2009). Currently, CCI is practised by various governments' security apparatus, a fast-growing number of corporates and a few cybersecurity vendors that offer such specialised services. Although CCI is integrated in the training curriculum of institutions such as military and intelligence academies, the curriculum content is not publically available. Furthermore, publically available literature on CCI in general and peer-reviewed academic research in particular remains very limited (Stech & Heckman 2018, Justiniano 2017). While a few commendable CCI frameworks/models have indeed been advanced, these frameworks/models expound very specific CCI aspects such as institutional maturity (Jaquire 2018), processes (Fieber 2015), training (Black 2014) and CCI's role in hybrid warfare (Justiniano 2017). These works do not attempt an overarching framework for structuring CCI as an emerging subdiscipline (Black 2014, Fieber 2015, Jaquire 2018, Stech & Heckman 2018). As matters currently stand, academic contributions to CCI are therefore not only scarce but – in the absence of an overarching framework – also conceptually fragmented. This scarcity of literature on CCI is further expanded on in Chapter 3.

So far, we have outlined the practical and academic need for a conceptual framework for CCI. This was followed by a very cursory overview of consulted literature which showed that, as far as could be ascertained, no such framework currently exists. This finding is central to the study's problem statement advanced in the next section.

1.2 PROBLEM STATEMENT AND RESEARCH QUESTIONS

In the preceding section, we positioned the design of a conceptual FCCI as a practical and academic imperative. Yet, at least in as far as the consulted literature is concerned, such an overarching framework does not exist.

This leads us to the primary **problem statement** of this research: In the literature studied, no overarching conceptual CCI framework that can provide a premise for establishing CCI as an academic subdiscipline, topic of instruction and research field could be found.

Flowing from the problem statement, the **central research questions** are threefold:

(1) What academically credible conceptual framework can be advanced to notionally structure CCI?

(2) What should the features and components of the framework be, and how should they be configured?

(3) Can conceptual constructs derived from Intelligence Studies (notably statutory intelligence and counterintelligence) be usefully applied to CCI and thus to the FCCI's design?

1.3 HYPOTHESES

The thesis's **primary hypothesis** is that an academic credible conceptual Framework for Cyber Counterintelligence can be designed by means of an inductive, qualitative methodology. By postulating the critical notional constructs which comprise CCI and by outlying the constructs' relations, the framework can narratively and graphically explain what CCI is and how it 'works'.

Accompanying the central hypothesis, the thesis' two **secondary hypotheses** are:

- Criteria can be formulated to derive the FCCI's features, components and configuration.
- Conceptual constructs from Intelligence Studies can be applied to CCI and utilised for the FCCI's design.

1.4 RESEARCH AIM AND OBJECTIVE

The study's main **aim** is to design an integrated conceptual framework for notionally structuring CCI as an emerging, multidisciplinary field of enquiry. This will be referred to throughout the thesis as the Framework for Cyber Counterintelligence (FCCI). For the purposes of this chapter, a 'conceptual framework' is tentatively defined as a construct which coherently explains – narratively and graphically – what CCI is, what its essential components are, how these components relate and thus how CCI 'works' (*cf.* Miles & Huberman 1994, Jabareen 2009). Such a framework will constitute a novel contribution which will add significantly to the very limited body of published academic knowledge in this field. Since it structures and adds to existing knowledge, our FCCI is intended to aid further research and theory building.

In pursuance of the primary aim, the study's **primary objective** is to construct the FCCI as a conceptual framework for notionally structuring CCI as an emerging, multidisciplinary field of enquiry. This construction will follow an inductive qualitative

methodology, within the realist paradigm, and will include an evaluative literature study to develop the FCCI and its components.

1.5 RESEARCH APPROACH AND STRUCTURE

In order to achieve the stated aim and objective, this thesis is divided into six parts.

Part 1, which consists of **Chapters 1 to 3**, lays the foundation for the design of our FCCI. To ensure the design of an academically credible FCCI, the notion of a 'conceptual framework' is examined in Chapter 2 to arrive at criteria with which the FCCI should comply. These criteria are then used to guide (a) the identification of the FCCI's main components and (b) an appropriate approach to design these components. In Chapter 3, we forward an evaluative literature study in order to (a) substantiate the problem statement and study objective, (b) position the thesis within the context of existing research, and (c) identify aspects in the literature useful to the construction to our FCCI.

Building on Part 1, in **Part 2** of the thesis, we advance our integrated FCCI and the reasoning behind its sequential block-by-block construction. Part 2 consists of one chapter, namely **Chapter 4**.

In **Part 3**, we discuss the eight building blocks of our FCCI and sequentially construct our FCCI. Part 3 consists of nine chapters (**Chapters 5–13**). The buildings blocks advanced in these chapters, which respectively and collectively explain what CCI is and how it works, are as follow:

- Building Block 1: Theoretical anchor
- Building Block 2: Organisation
- Building Block 3: Intelligence
- Building Block 4: Counterintelligence
- Building Block 5: Cyber Counterintelligence
- Building Block 6.1: Cyber Counterintelligence Matrix – Horizontal plane
- Building Block 6.2: Cyber Counterintelligence Matrix – Vertical plane
- Building Block 7: Delineation
- Building Block 8: Cyber Counterintelligence Process

Part 4 applies the FCCI (constructed in Part 3) as an organisational training concept. Practically, this entails a high-level proposition on utilising the FCCI as a tool in an

organisation's CCI training and awareness programme. Part 4 consists of one chapter, namely **Chapter 14**

In **Part 5**, we conclude the thesis with **Chapter 15** by assessing the research questions, testing the hypotheses, appraising the FCCI research's significance and proposing areas for further CCI research**.**

In summary, the thesis's chapter division (which is discussed further in Section 2.3 of Chapter 2) is as follows:

Table 1: Structure of the thesis (Author)

PART 1: FOUNDATION AND CONFIGURATION OF THE FRAMEWORK FOR CYBER COUNTERINTELLIGENCE		
Chapter 1	Introduction	In these chapters, the need for and purpose of our FCCI are motivated. We explain the essential features of a conceptual framework to which our FCCI should comply as well as the methodological approach required to construct an academically credible FCCI.
Chapter 2	Features and Configuration of the Conceptual Framework for Cyber Counterintelligence	
Chapter 3	Evaluative Literature Study	
PART 2: OVERVIEW OF THE INTEGRATED FRAMEWORK FOR CYBER COUNTERINTELLIGENCE – BLUEPRINT AND DESIGN LOGIC		
Chapter 4	Overview of the Integrated Framework for Cyber Counterintelligence	This part is a high-level overview of our integrated FCCI. By means of graphics, the FCCI's eight building blocks and the synergy between these blocks are shown. The integrated FCCI is, by way of analogy, the 'blueprint' of the thesis, the end-product of the research. It can, also by of way of comparison, be seen as the 'final destination' of the research. As a supplement to the blueprint, the design logic concisely explains the reasoning behind the FCCI's block-by-block construction. This design logic is thus a cursory step-by-step 'construction manual' to guide the reader to the final destination.

PART 3 : EXPLICATION OF THE BUILDING BLOCKS OF THE FRAMEWORK FOR CYBER COUNTERINTELLIGENCE		
Chapter 5	Building Block 1: Theoretical Anchor	In these chapters, the various aspects that respectively and collectively explain what CCI is, and how it works, are described.
Chapter 6	Building Block 2: Organisation	
Chapter 7	Building Block 3: Intelligence	
Chapter 8	Building Block 4: Counterintelligence	
Chapter 9	Building Block 5: Cyber Counterintelligence	
Chapter 10	Building Block 6.1: CCI Matrix – Horizontal plane	
Chapter 11	Building Block 6.2: CCI Matrix – Vertical plane	
Chapter 12	Building Block 7: Delineation	
Chapter 13	Building Block 8: Cyber Counterintelligence Process	
PART 4: THE FCCI AS AN ORGANISATIONAL TRAINING TOOL		
Chapter 14	The FCCI's as an Organisational Training Tool	This chapter explores the FFCI's application as a tool for an organisation's CCI training and awareness programme.
PART 5: CASE STUDY, EVALUATION AND CONCLUSION		
Chapter 15	Evaluation and Conclusion	Here the problem statement, research questions and hypotheses are evaluated, and areas for further research on CCI are highlighted. Given the requirements for a doctoral thesis, we also observe on our FCCI's research's significance.

In this section, we explained the structural approach of the study by outlining the five parts and the different chapters which comprise the thesis. In the next section, papers

and articles leading up to and flowing from our research to design our FCCI are discussed.

1.6 RESEARCH LEADING UP TO AND FLOWING FROM THE THESIS

This thesis forms part of a CCI research project at the University of Johannesburg's Centre for Cyber Security. Details of this project can be viewed on the centre's website at http://www.cybersecurity.org.za. **Peer-reviewed papers and articles** published and leading up to the thesis are:

- Duvenage, P.C. & von Solms. S.H. (2013) 'The case for cyber counterintelligence' in *Published Proceedings of the 5th International Workshop on ICT Uses in Warfare and the Safeguarding of Peace,* Institute of Electrical and Electronic Engineers (IEEE), Pretoria, South Africa, November (See **Annexure A**).
- Duvenage, P.C. & von Solms. S.H. (2014) 'Cyber counterintelligence: Putting counterintelligence in cyber counterintelligence' in *Published Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece, July (See **Annexure B**).
- Duvenage, P.C. & von Solms. S.H. (2015) 'Cyber counterintelligence: Back to the future', *Journal of Information Warfare*, 13(4):42–56 (See **Annexure C**).
- Duvenage, P.C., von Solms, S.H. & Corregedor, M. (2015) 'The cyber counterintelligence process – A conceptual overview and theoretical proposition' in *Published Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK, July (See **Annexure D**).
- Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2016) 'Conceptualising cyber counterintelligence – Two tentative building blocks' in *Published Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, Germany, June (See **Annexure E**).
- Duvenage, P.C., Sithole, T.G. & von Solms, S.H. (2017) 'A conceptual framework for cyber counterintelligence – Theory that really matters' in *Published Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland, June (See **Annexure F**).
- Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2018a) 'A selective literature review on cyber counterintelligence' in *Published Proceedings of the 17th*

European Conference on Cyber Warfare and Security, Oslo, Norway, June (See **Annexure G**).

- Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2018b) 'Towards a literature review on cyber counterintelligence' in *Journal of Information Warfare*, 17(4): 11-25 (See **Annexure H**).
- Jaquire, V.J., Duvenage, P.C. & von Solms, S.H. (2018) 'Building the CCI dream team' in *Published Proceedings of the 17th European Conference on Cyber Warfare and Security*, Oslo, Norway, June (See **Annexure I**).
- Sithole, T.G., Duvenage, P.C., Jaquire, V.J. & von Solms, S. H. (2019) 'Eating the elephant – A structural outline of cyber counterintelligence awareness and training' in *Published Proceedings of the 14th International Conference on Cyberwarfare and Security,* Stellenbosch, South Africa, February (See **Annexure J**).
- Duvenage, P.C., Jaquire, V. J. & von Solms, S.H. (2019) 'A cyber counterintelligence matrix for outsmarting your adversaries' in *Published Proceedings of the 18th European Conference on Cyber Warfare and Security*, Coimbra, Portugal, July (See **Annexure K**).
- van Niekerk, B., Ramluckan, T. & Duvenage, P.C. (2019) 'An analysis of selected cyber intelligence texts' in *Published Proceedings of the 18th European Conference on Cyber Warfare and Security*, Coimbra, Portugal, July (See **Annexure L**).

This thesis is categorically qualified as relying for content on, and as containing verbatim extracts, from the above-mentioned research. However, to arrive at the coherent FCCI presented in the thesis, we not only consolidated previous research – which include several original CCI constructs – but also offer substantial further syntheses as well as further novel contributions. [1]

In addition to the peer-review of the research outlined above, some key aspects of the thesis were included in papers/presentations on CCI at **pre-eminent, non-academic events** for information technology (IT) executives and practitioners. While the proceedings of these events were not published and academically peer reviewed[2],

[1] The author's contributions to the above listed research are quantified per "Annexures" on pages 194 – 195.

[2] Since the proceedings of these events were not published and formally peer reviewed, they are not included in the thesis's reference section.

verbal and other interaction during these events were invaluable in configuring the FCCI's design to practice. These events included:

- Van Niekerk, B. & Duvenage, P.C. (2016) 'Cyber intelligence and counterintelligence', *Information System Control and Audit Association (ISACA) Annual Conference* (South African Chapter), Kempton Park, South Africa, August.
- Duvenage, P.C. (2015) 'Cyber counterintelligence – The silver bullet?', *GovCon/ AfricaCon*, South African Government, Pretoria, South Africa, November.
- Duvenage, P.C. & von Solms, S.H. (2014) 'Cyber counterintelligence – What is it and what has recent history taught us?', *IT Web Security Summit*, Sandton, South Africa, May.
- Duvenage, P.C. & von Solms, S.H. (2013) 'Business cyber counterintelligence', *(ISC)^2 Secure Johannesburg Conference*, Johannesburg, South Africa .

Throughout the thesis, CCI is emphasised and explained as an integral part of **multidisciplinary CI**. To this end, this thesis draws on, and contains extracts from, the following peer-reviewed contributions on CI by the author:

- Duvenage, P.C. (2013) 'Counterintelligence' in Prunckun, H. (ed.), *Intelligence and private investigation: Developing sophisticated methods for conducting inquiries*, Charles C. Thomas Publishers, Illinois, US.
- Duvenage, P.C. & Hough, M. (2011) 'The conceptual structuring of the intelligence and the counterintelligence processes: Enduring holy grails or crumbling axioms – Quo vadis?' in *Strategic Review for Southern Africa,* 33(1).
- Duvenage, P.C. (2011) *Open-source environmental scanning and risk assessment in the statutory counterespionage milieu*, unpublished DPhil thesis, University of Pretoria, Pretoria, South Africa.

In this section, we highlighted completed and ongoing research by the author drawn on for this thesis. In the next section, the chapter is summarised and concluded.

1.7 SUMMARY AND CONCLUSION

In this chapter, we introduced the primary problem statement, research questions and hypotheses of the study. The dire practical and academic need for an FCCI was emphasised. We argued that an FCCI is essential for establishing CCI as an academic subdiscipline, a topic of instruction and a research field. Moving from the hypothesis

that the FCCI can be constructed by inductive qualitative means, we outlined the basic structural approach to be followed. We then proceeded to highlighting peer-reviewed research drawn on for this thesis.

To ensure that the FCCI we construct is academically credible, we have to be clear regarding what a conceptual framework is and what its features are. These aspects are examined in the next chapter.

CHAPTER 2

FEATURES AND CONFIGURATION OF THE FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

2.1 INTRODUCTION

In Chapter 1, the study's problem statement, research questions, hypotheses, research objective and approach were advanced. In this chapter, the primary objective of the study, namely the design of our conceptual FCCI, is further unpacked and concretised.

To be academically credible, the design of our FCCI needs to be clear in terms of what a conceptual framework **is**, what it should **consist** of and what it should **do**. In the interest of simplicity, these three questions are reduced to one central question that will guide the **first content part of this chapter (Section 2.2)**, namely what **are the features that the FCCI should have**? To address this central question, in Section 2.2 we move from an examination of the notion of a conceptual framework in general to pertinent features that our FCCI should have. To this end, Section 2.2 comprises the following:

- Subsection 2.2.1: Context 1 – Features of a conceptual framework as a qualitative research design tool
- Subsection 2.2.2: Context 2 – Features of the conceptual framework as a construct aiding multidisciplinary research
- Subsection 2.2.3: Context 3 – Features of the conceptual framework centred on Cyber Counterintelligence as an emerging Intelligence Studies field
- Subsection 2.2.4: Integrated postulation on the criteria for a framework for Cyber Counterintelligence

In the **second content part of this chapter (Section 2.3)**, the features identified above are used as criteria to configure the design of the FCCI. Practically, this entails using the identified criteria to (a) determine the FCCI's components and (b) configure an academically credible approach to construct these components. These components are then discussed in subsequent chapters of this thesis by means of a tabulated outline. This outline is presented in **Section 2.3** with the heading "Configuring our conceptual framework for cyber counterintelligence". Graphically, we can map the chapter's flow as follows:

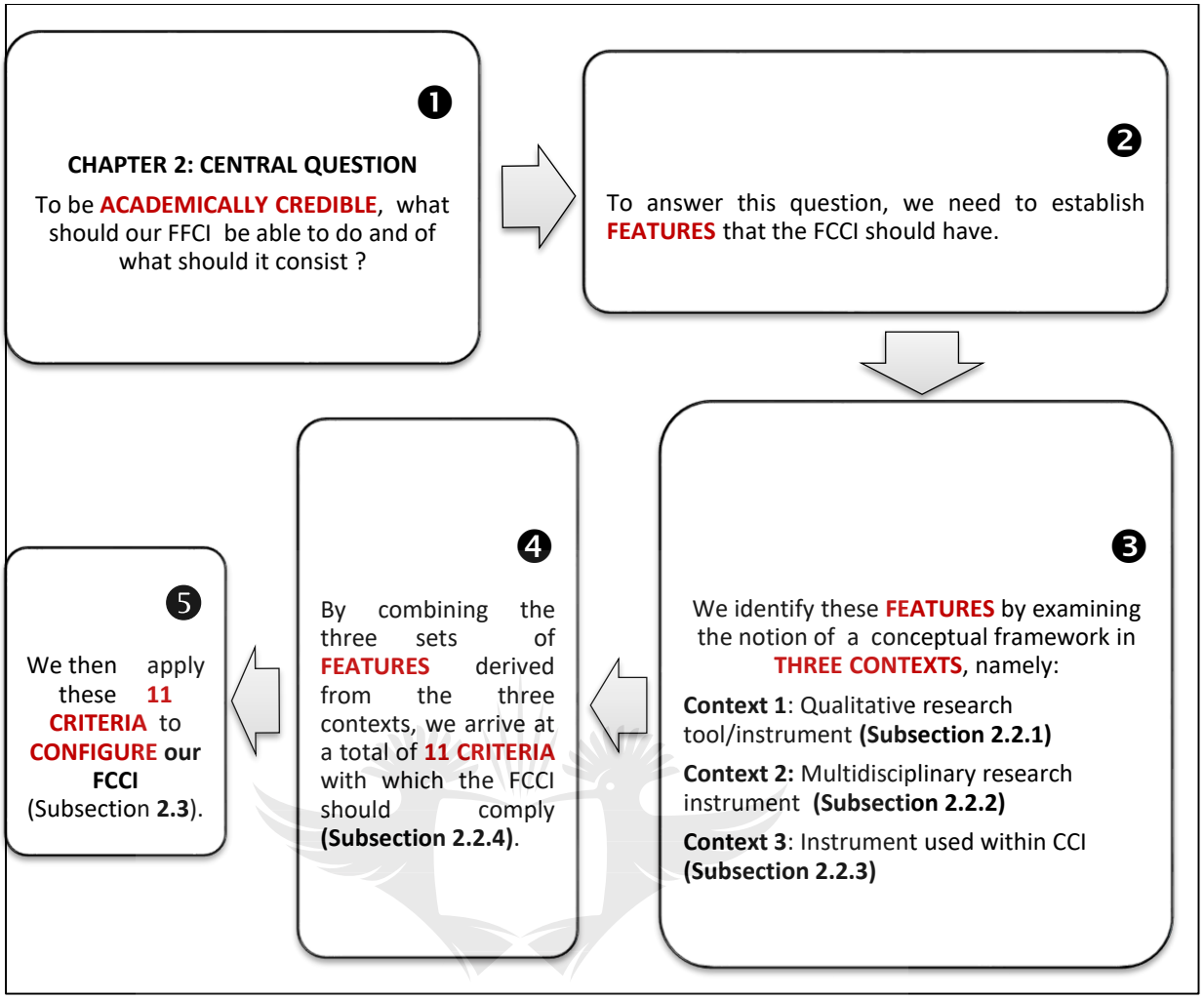


Figure 1: Layout and logic of Chapter 2 (Author)

In this section, we discussed our approach to the chapter. In the next section, the notion of a conceptual framework is examined in three contexts (❸ in Figure 1) in order to identify features and then arrive at criteria (❹ in Figure 1) with which the FCCI should comply.

2.2 FEATURES OF A CONCEPTUAL FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

Given the infancy of CCI as an academic field, it is unsurprising that no reference to criteria for an FCCI could be found in the literature we consulted. Consequently, such requirements have to be derived by first looking at conceptual frameworks and their characteristics in other contexts. To this end, we follow a funnel approach in examining

conceptual frameworks within three contexts, moving from the general to the specific. After each subsection, features for the FCCI are deduced.

2.2.1 CONTEXT 1: FEATURES OF A CONCEPTUAL FRAMEWORK AS A QUALITATIVE RESEARCH DESIGN TOOL

In the literature that we consulted, the term 'conceptual framework' is widely used as referring to a notional construct in the design and structuring of qualitative research – notably master's and doctoral studies. In this context, the term 'conceptual framework' denotes a tentative postulation which combines the ideas around, and dimensions of, a phenomena that is to be researched. Smyth (2004) concisely defines a conceptual framework as "a conception or model of what is out there that you plan to study". Maxwell (2012) describes a study's conceptual framework as the "system of concepts, assumptions, expectations, beliefs, and theories that supports and informs your research." Similarly, Miles and Huberman (1994) posit a conceptual framework as a visual or written product which "explains, either graphically or in narrative form, the main things to be studied – the key factors, concepts, or variables – and the presumed relationships among them". While these definitions differ in exact wording, they all convey the idea of a conceptual framework as a preliminary construct which combines various components (concepts, factors, theories, etc.) and provides a coherent view of the research object. A conceptual framework is, in other words, both an overarching concept that binds underlying concepts (ideas, concepts, factors, theories, etc.) and the collective of the overarching and the underlying concepts.

In addition to tentatively delineating the referent object (what is going to be studied), a conceptual framework advances initial explanations as to "what is going with these things and why" (Maxwell 2012). While existing theories and research are considered in its design, a sound conceptual framework thus adds insights. In this regard, Maxwell (2012) states: "…a conceptual framework for your research is something that is constructed, not found. It incorporates pieces that are borrowed from elsewhere, but the structure, the overall coherence, is something that you build, not something that exist ready-made."

The abovementioned insights a conceptual framework provides attest to its value as a **qualitative research design tool** which directs initial research phases (Smyth 2004). Early in the research process, a conceptual framework aids the development of relevant research questions, the selection of research methods and managing validity threats to the research project (Maxwell 2012). Insights the conceptual framework

provide regarding the deficiencies of existing research could, for example, guide the formulation of both research goals and research questions. Research questions, in turn, determine research methods and the validity of research. Maxwell (2012) depicts this relation between a conceptual framework and other aspects of research design as follows:

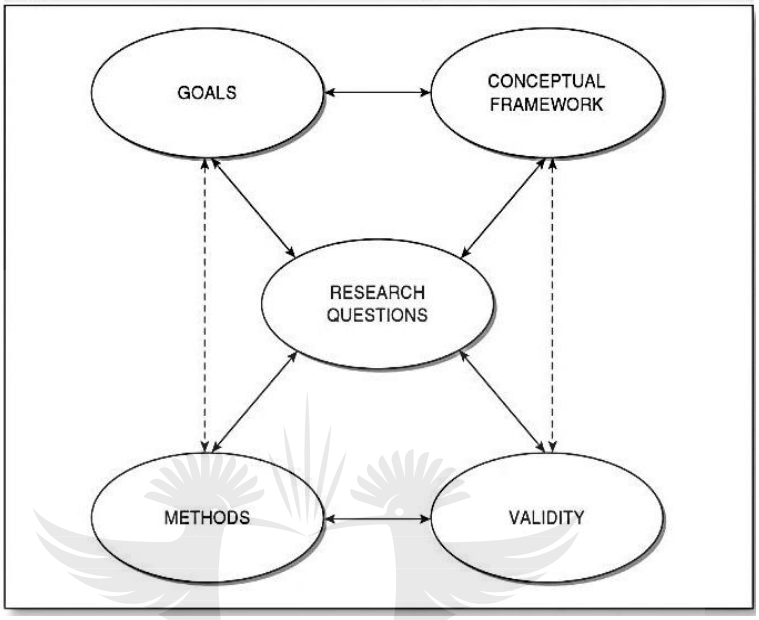


Figure 2: Interactive Model of Research Design (Maxwell 2012)

Since a conceptual framework delineates concepts and posits relationships between them, the conceptual framework is in itself a tentative theory. If used as a **qualitative design tool** in the early stage of research, a conceptual framework has as primary sources (1) the researcher's experiential knowledge, (2) existing theory and research, (3) pilot and exploratory research, and (4) "thought experiments" which include synthesis and speculative model building (Maxwell 2012, Smyth 2004).

While the FCCI advanced in this thesis is indeed exploratory in nature, it is the end result of a doctoral study and not a design tool for pilot research. Consequently, we cannot summarily and unqualified apply the characteristics of a conceptual framework (in the context of a pilot research design tool) to the FFCI. Nonetheless, the foregoing discussion does convey generic characteristics which transcend specific contexts and can thus be applied with circumspection to the FCCI. With this qualification, we can state that a qualitative conceptual framework generally would have the following features:

- The framework advances an overall schema which delineates a study object or field. This schema synthesises underlying concepts to provide a coherent view of the study object.
- It has as components both the overarching schema and underlying (constituent) concepts. These constituent concepts describe the research object's salient facets.
- It describes components narratively and/or visually. Constructs aiding such narrative/visual description include definitions, classifications, diagrams, taxonomies and models.
- It postulates the links and relations between the concepts.
- It is derived through a qualitative process which draws on the researcher's experiential knowledge, existing theory and research, as well as new research and theory.

In this section, we examined the notion of a conceptual framework in the **context of a qualitative research design tool** and derived certain features which the FCCI should have. A central finding is that a conceptual framework's components could consist of an overarching schema and constituent concepts (which can be presented visually and narratively). In the next section, we examine a conceptual framework within the context of multidisciplinary research.

2.2.2 CONTEXT 2: FEATURES OF THE CONCEPTUAL FRAMEWORK AS A CONSTRUCT AIDING MULTIDISCIPLINARY RESEARCH

The use of a conceptual framework is of course not limited to that of a research design tool. The creation of a conceptual framework can also be the final outcome (end product) of research activities which range from papers and articles to master's and doctoral studies. This doctoral study is a case in point. Such 'end-product' conceptual frameworks are proving particularly useful in contemporary research which increasingly deals with phenomena that are intrinsically interdisciplinary or multidisciplinary (Junghans & Olsson 2012). Since the FCCI deals with a field which (as will be shown in Chapters 7 and 8) is intrinsically multidisciplinary, the application of conceptual frameworks within **the context of multidisciplinary research** and the implications thereof for the FCCI's design warrant further examination.

It is important to note that the notion 'conceptual framework' retains its core meaning when applied to the multidisciplinary 'end-product' context. This is clear from the following definition provided by Jabareen (2009) in a multidisciplinary setting: "A [c]onceptual framework is…a network, or a 'plane' of interlinked concepts that together

provide a comprehensive understanding of a phenomenon or phenomena...Conceptual frameworks are not merely collections of concepts but, rather, constructs in which each concept plays an integral role." More often than not, multidisciplinary phenomena "do not even have a skeletal framework" that can logically structure academic enquiry (Jabareen 2009). Therefore, there is a need for a notional structure which can on the one hand systemise existing knowledge (literature) and on the other hand direct further multidisciplinary academic enquiry (Junghans & Olsson 2012). A properly constructed conceptual framework can fill this void by establishing a 'scaffold' for evolving research (*cf.* Smyth 2004).

Compared to the use of a conceptual framework as a research design tool (discussed in Subsection 2.2.1), producing a multidisciplinary framework as the end product is considerably more extensive and meticulous. Typically a qualitative methodology is followed. In the case of a multidisciplinary conceptual framework, such a qualitative methodology could consists of the following phases: (1) mapping of sources (2) extensive survey and categorisation of data (3) identification and naming of concepts, (4) deconstruction and categorisation of concepts (5) integration of concepts, (6) synthesis of concepts in a framework, (7) validating the framework, and (8) dynamical revision and modification of the conceptual framework (Jabareen 2009). As will be observed, this methodology entails creating new concepts through a process of considering but moving beyond existing thinking. Through this process, existing concepts are reconfigured and where applicable new ones are created.

While the compilation of a conceptual framework involves theorisation, it is important that it also takes into account and reflect real-world practice (Junghans & Olsson 2012, Jabareen 2009). When the phenomenon being studied is linked to a profession or professions, the need for a conceptual framework to be synchronised with practice is even more imperative (*cf.* Junghans & Olsson 2012). Essentially it can be stated that practice should inform theory and theory should be relevant to practice.

We can deduct from the discussion above that a **conceptual framework within the multidisciplinary context** has the following features:

- A specific research area is demarcated and a comprehensive understanding thereof is provided.
- Existing concepts are considered but also surpassed by designing novel constructs. Therefore, a framework's building blocks comprise existing concepts, reconfigured concepts and new constructs.

- Existing knowledge and literature are structured in a manner conducive to further research.
- The practice(s) of the related profession(s) are accounted for and reflected.
- It is an artefact subject to modification.

In this section, we examined the requirements for a conceptual framework within the context of multidisciplinary research. In the next section, features stemming from the FCCI's location within CCI as an emerging field of enquiry are identified.

2.2.3 CONTEXT 3: FEATURES OF THE CONCEPTUAL FRAMEWORK CENTRED ON CYBER COUNTERINTELLIGENCE AS AN EMERGING INTELLIGENCE STUDIES FIELD

In Part 2 of this thesis, we show that although CCI is multidisciplinary in nature, its primary **conceptual taproots** are in the academic discipline of Intelligence Studies. As suggested by the term itself ('cyber **counterintelligence**'), CCI is more specifically located within the Intelligence Studies specialisation area of counterintelligence (CI). On a conceptual level, CCI concerns the application of CI constructs and principles to the cybersphere. On the level of practical execution, however, CCI is simultaneously very much dependent on the cyber-related disciplines of computer science and informatics. Since we focus here on deriving features on a conceptual level, CCI's location within CI and Intelligence Studies is pertinent.

The fact that our FCCI deals with an emerging field (CCI) within a discipline (Intelligence Studies) poses challenges arising from demarcating a crystallising academic subject. This has four interrelated implications for the design of the conceptual framework.

(1) The framework has to duly consider existing intelligence/CI theoretical constructs and concepts when deriving the components of the FCCI. As stated in Section 2.2, this does not imply that existing constructs are merely 'copied' and applied to the FCCI. Rather, existing constructs should be considered and evaluated, and those of value ought be refined or incorporated in novel concepts that explain CCI.

(2) The FCCI has to clearly position CCI as a notional subset of intelligence and CI. Apart from conceptual clarity, such positioning also has the utility of interlocking CI and CCI when it comes to the practical execution of these functions.

(3) As implied in the last statement, the FFCI's design has to compute the fact that Intelligence Studies is the academic complement to the CI profession which has

CCI as a rapidly expanding specialisation field. Therefore, the FCCI as a theoretical artefact should not be about the generation of theory for theory's sake. It should, to reiterate the point made in Section 2.3, reflect practice. While a conceptual framework is not a 'manual' to a profession, it ought to be more than abstract theory. Ultimately such frameworks condition our thinking and our approach to practice (*cf.* Duvenage & von Solms 2013). Thus, the FCCI's components should be selected and designed to sufficiently explain how CCI works.

(4) To aid CCI's evolvement as an academic field, the FCCI has to provide a scaffold for organising "accumulated specialist knowledge effectively" (Krishnan 2009).

From the aforementioned, we can assert that **a conceptual framework within the context of CCI as an emerging intelligence and CI field** have the following features:

- It notionally and concretely positions CCI as a subset of intelligence and CI.
- On a theoretical level, it draws on Intelligence Studies with due consideration of the imperatives posed by the practical execution of CCI which relies on the computer science and informatics disciplines.
- It selects and designs components that explain how CCI works.
- It provides a premise for organising accumulating subject knowledge effectively.

In this section, we derived features from the conceptual framework's focus on CCI as an emerging Intelligence Studies field. In the next section, we present a consolidated postulation on the criteria with which the FCCI should comply.

2.2.4 INTEGRATED POSTULATION ON THE CRITERIA FOR A FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

Thus far in this chapter, we inferred features of a conceptual framework from three contexts that vary from the general to the specific. In order to be useful for our FCCI's design, features from these different contexts have to be integrated and applied to our FCCI. In so doing, the features constitute criteria with which our FCCI should comply. In the interest of simplicity, we then cluster the criteria according to those pertaining to the purpose of our FCCI and those dealing with its components and design. Accordingly, this subsection consists of the following:

2.2.4.1. Criteria pertaining to the purpose of the FCCI.

2.2.4.2. Criteria for the components and design of the framework for FCCI.

To enable easier reference later in this chapter (Section 2.3, Table 2), criteria are not numbered per subsection but by following **a continuous numbering format (1–11)**.

2.2.4.1 Criteria pertaining to the FCCI's purpose

Flowing from the above, the following can be postulated as **criteria** with which the FCCI's purpose should comply:

(1) Provide a comprehensive and coherent understanding of what CCI is, of what it comprises and how it works.

(2) Serve as a conceptual template for modelling CCI practice and its synergetic execution with broader CI.

(3) Contribute to establishing CCI as an academic field. This should be done with due reference to its relation with intelligence and CI as well as with computer science and informatics.

(4) Establish a premise for organising accumulating CCI subject knowledge.

2.2.4.2 Criteria for the FCCI's components and design

The FCCI's effectiveness in attaining its purpose depends on a sound design which identifies, incorporates and links various conceptual constructs (components). In respect of its components, the FCCI is required to:

(5) Advance an **overarching schema** which narratively and/or graphically provides a coherent understanding of CCI. The schema must establish a notional nexus which not only binds the framework's constituent components, but interlocks CCI with CI.

(6) Contain **constituent concepts** (building blocks) that describe salient CCI aspects. Whereas the overarching schema is pitched at a theoretical level of higher abstraction, constituent concepts should be more concrete in that they reflect CCI practice. It must explain more concretely what CCI is and how it works. Practically this means that constituent parts should explain CCI **tools, processes, execution and postures**.

(7) Describe components **narratively** and, if possible, **visually**. Constructs aiding such narrative/visual description should include definitions, classifications, diagrams, taxonomies and models.

(8) In support of the overarching schema, provide additional postulations which explain the **links** between the various constituents as well as CCI's interlock with existing theory, intelligence and CI.

(9) In the design of components, consider but also **move beyond existing concepts** by designing novel constructs. Therefore, a framework's building blocks could comprise existing concepts, reconfigured concepts and new constructs.

(10) Be derived at through a **qualitative process** which draws on the researcher's experiential knowledge, existing theory and research as well as new research and theory.

(11) Be qualified as a **tentative artefact** that is subject to validation and constant modification.

This section concludes the first part of the chapter which is aimed at formulating criteria for the FCCI's design. This was done through an examination of the notion of a conceptual framework in different contexts. Using these features and applying them to CCI, we inferred 11 specific criteria for an FCCI. In the next section, we employ these criteria to design and configure our FCCI in an academically credible manner.

2.3 CONFIGURING OUR CONCEPTUAL FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

In the preceding section, **11 criteria** with which the FCCI should comply were forwarded. These criteria are critical since they provide a footing for designing an FCCI that is academically sound. Using these criteria as a yardstick, we can proceed to identify concepts that are essential in explaining and notionally structuring CCI. In practical terms, these concepts are our FCCI's components, **which are twofold:**

(1) An **overarching schema** (i.e. the integrated FCCI – Chapter 4), and

(2) **Building blocks** (i.e. the individual components of the FCCI – Chapters 5-13)

We arrange these components in a logically sequential manner in chapters. The outcome of this process is an outline of our FCCI's configuration as provided in Table 2 below. To ensure that our FCCI is academically credible and grounded, in the table's '**Criteria Met**' column, these building blocks are measured against the **11 criteria** arrived at in Subsection 2.2.4. This is done by referring to the numbers assigned to the criteria.

Table 2: Outline of the FCCI's Configuration (Source: Author)

CHAPTER	DESCRIPTION	CRITERIA MET
PART 1: FOUNDATION AND CONFIGURATION OF THE FCCI		
1	Introduction	Not applicable.
2	Features and Configuration of the FCCI	
3	Evaluative Literature Study	**3, 4, 10**
PART 2: OVERVIEW OF THE INTEGRATED FCCI – BLUEPRINT AND DESIGN LOGIC		
4	Overview of the integrated FCCI	**1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11**
PART 3 : EXPLICATION OF THE FCCI's BUILDING BLOCKS		
5	Building Block 1: Theoretical Anchor	**2, 3, 4, 6, 7, 8, 9, 10**
6	Building Block 2: Organisation	
7	Building Block 3: Intelligence	
8	Building Block 4: Counterintelligence	
9	Building Block 5: Cyber Counterintelligence	
10	Building Block 6.1: CCI Matrix – horizontal plane	
11	Building Block 6.2: CCI Matrix – vertical plane	
12	Building Block 7: Delineation	
13	Building Block 8 : CCI Process	
PART 4: THE FCCI AS AN ORGANISATIONAL TRAINING TOOL		
14	The FCCI's as an Organisational Training Tool	**2, 3, 4, 6, 7, 8, 9, 10**
PART 5: CASE STUDY, EVALUATION AND CONCLUSION		
15	Evaluation and Conclusion	**3, 4, 10, 11**

This section gave practically effect to the criteria with which the FCCI should comply by presenting a tabulated configuration of the framework. Table 2 shows that the FFCI complies with the **11 criteria** which an academically credible FCCI should meet.

2.4 SUMMARY AND CONCLUSION

This chapter's primary aim was to concretise the study's primary objective, namely designing an academically credible FCCI. To achieve this aim, the approach to and design of the FCCI have to comply with academically justifiable criteria. To this end, we examined the notion of a conceptual framework in **three contexts** to identify salient **features**. These features were consolidated and applied to CCI, thereby arriving at a consolidated list of **criteria**. We then used these criteria to evaluate the academic credibility of the FCCI's components, consisting of the integrated FCCI (overarching schema) and its building blocks. In the next chapter, we provide an overview of the relevant literature with the aim of establishing a structured base for our research.

CHAPTER 3

EVALUATIVE LITERATURE STUDY

3.1 INTRODUCTION

In the preceding chapter, we concretised the study's primary objective (namely the design of our FCCI). We alluded to the requirement that our FCCI should be based on, and move beyond, existing research and thinking. This research and thinking are of course reflected in existing literature on CCI. The primary aim with Chapter 3 - which incorporates Duvenage, Jaquire & von Solms 2018a, 2018b - is to offer an evaluative study of CCI literature. To this end, the chapter comprises:

- Section 3.2, which details the purpose and importance of an appraisal of CCI literature
- Section 3.3, where we qualify the scope and nature of the literature review
- Section 3.4, which explains the structural approach to the literature review
- Sections 3.5 - 3.8, where CCI contributions are assessed in the following categories:
  - Section 3.5: Academic papers and articles
  - Section 3.6: Master's and doctoral studies
  - Section 3.7: Books
  - Section 3.8: Other literature

In this section, we introduced the chapter's aim and outlined the approach we will follow. In the next section, we examine the purpose and importance of a CCI literature review.

3.2 PURPOSE AND IMPORTANCE OF A LITERATURE REVIEW ON CYBER COUNTERINTELLIGENCE

Although a literature review is a standard component of dissertations and theses, such an appraisal is of particular importance for the design of our FCCI for the following reasons:

- The study's problem statement and primary objective are premised on the assertion that in consulted literature, there is no overarching, conceptual CCI

framework. The literature review, which is more comprehensive than the cursory overview in Chapter 1 (Section 1.1), is aimed at corroborating our assertion about the current lack of an FCCI. In other words, a comprehensive literature review is necessary to **substantiate the problem statement and objective of the study**.

- In Chapter 2 (Subsection 2.2.4 – Criteria for the FCCI's components and design) a qualitative methodology that includes an **evaluative literature study** was identified as a requirement for our FCCI to be **academically credible**.
- The contextualisation of the study against existing CCI research is necessary to substantiate the assertion that this doctoral thesis constitutes a **significant contribution** to the study field.
- Since CCI is an emerging field, with a relatively limited body of knowledge, a selective assessment of existing literature is realistically feasible and can provide a **'scaffold'** for positioning this study and adding future contributions to this field. This scaffold will thus complement our FCCI in **structuring existing knowledge** in a manner conducive for further research.
- Because it deals with salient research done thus far, a literature review offers an insight into CCI's academic origin, emergence and development. In doing so, a literature view could provide some contours of CCI's history. Observing on ICT and cybersecurity more generally, Caelli, Liu and Longley (2013) state:

> For any discipline to be regarded as a professional undertaking by which its members may be treated as true "professionals", practitioners must clearly understand that discipline's history as well as the place and significance of that history in current practice as well as its relevance to available technologies and artefacts at the time.

This is also true for CCI. As is the case with other academic subjects, the historic **self-awareness** a literature overview provides could thus contribute to consolidating CCI as a distinctive subdiscipline.

- As the literature review identifies research projects/institutions focused on CCI, it could aid academic interaction in this field.

In this section, we discussed the purpose and importance of a literature review on CCI. In the subsequent section, we stipulate some qualifications to the review.

3.3 QUALIFYING THE SCOPE AND NATURE OF THE LITERATURE REVIEW

While a comprehensive literature review is necessary, it is not the study's primary aim. Therefore, and within the confines a thesis chapter, the review is explicitly qualified as being a **'selective'** assessment of **'available'** literature. In line with this qualification, the literature review we advance in this chapter limits its focus in the following five respects:

(1) 'Available literature' is deemed as works in the public domain. Due cognisance is taken of the fact that state security structures internationally generate and possess CCI-relevant research and training material, of which some are unclassified, but not freely available. The same applies to some corporate entities and cybersecurity vendors which, for various considerations, do not openly share CCI material. Such material is categorically excluded from this review.

(2) 'Available literature' is secondly deemed as referring to work published in English. Although cursory reference will be made to a few works in other languages, the search which informed the review did not purposefully cover untranslated CCI-research.

(3) The literature review is furthermore 'selective' in that it predominantly focuses on material which explicitly addresses CCI. While overlapping themes (such as cyber denial and deception, insider threat mitigation, cyber intelligence and cyber threat intelligence) are important to CCI, a review of such literature would distract from the chapter's aim.

(4) The literature review is 'selective' in that it does not purport be an inventory of all CCI-focused work in English. Instead, in terms of academic works the review reflects on peer-reviewed, published work featured in selected platforms, namely: Scopus, EBSCO, Institute of Electrical and Electronics Engineers (I.E.E.E.E.) Explore, Springer Link, Google Scholar and Proquest.

(5) Lastly, the literature review only covers salient contributions published up to Augusts 2018.

Moving from the foregoing calibration of the CCI literature overview's selective scope, the next section explains the structural approach to be followed.

3.4 STRUCTURAL APPROACH TO THE LITERATURE REVIEW

A literature review should, of course, be structured in a manner optimally achieving its purpose and benefits. Given this literature review's earlier stated purpose and benefits (Section 3.2), we considered a structuring *per* either (a) literature category or (b) chronologically – that is, in order of publication. On the one hand, the conventional approach of dividing reviews per literature category (for example, articles, master's and doctoral studies, books) would arguably be the best suited to plot existing, and to provide a scaffold for positioning future, CCI research. On the other hand, a chronological literature review would be more effective to convey CCI's academic origin and development. To draw on the advantages both these options offer, we opted for a hybrid approach which incorporates a chronological thread with literature type. Practically, this means that the review is structured overall *per* the literature categories, namely peer-reviewed articles and papers, master's and doctoral studies, books and other literature. However, and since the bulk of CCI academic work was produced *per* peer-reviewed articles and papers, this literature category (i.e. peer-reviewed articles and papers) is presented chronologically in order to so convey CCI's origin and evolution. Where necessary for chronological coherence, our discussion of 'peer-reviewed articles and papers' will also refer to publications from other literature types. This hybrid structural approach to the selective CCI literature review is depicted in Figure 3.

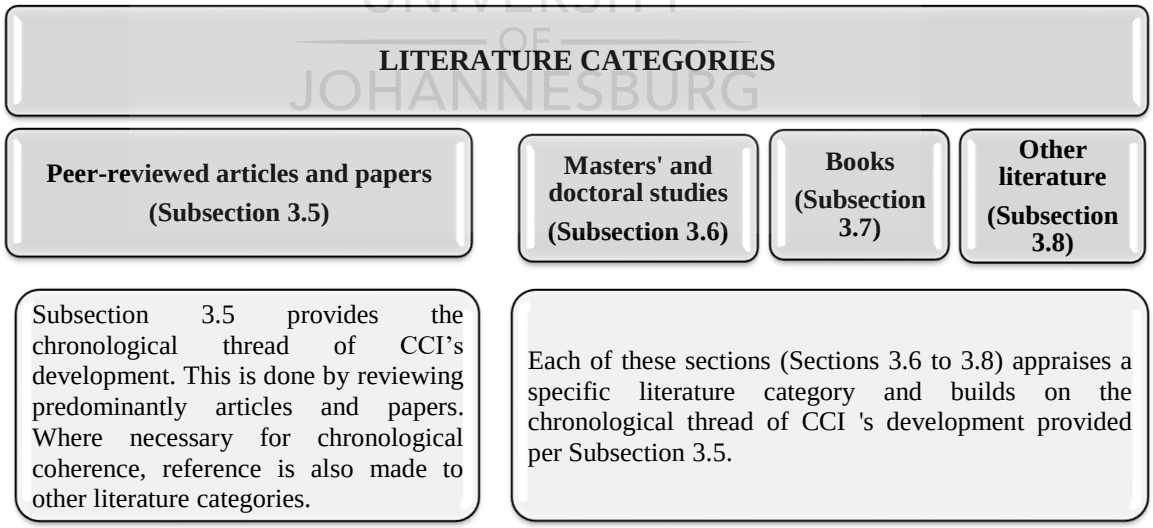


Figure 3: Structural Approach to the Literature Review on CCI (Adapted from Duvenage, Jaquire & von Solms 2018b)

Thus far in the chapter, we have discussed the CCI literature review's purpose, scope and the approach to be followed. In accordance, with the discussed approach we now proceed with discussing CCI literature *per* category.

To assist the reader in tracking the direct relevance of literature to our FCC's design, **FCCI** will be highlighted in **red bold font** in **Sections 3.5 – 3.8**, pages 30 - 41.

3.5 PEER-REVIEWED ARTICLES AND PAPERS

In line with Figure 3, this Section contours CCI's evolvement with specific reference to peer-review articles and papers. Although somewhat of an over-simplification, CCI's progression as a distinctive academic subdiscipline consists of the following phases:

- Subsection 3.5.1: Foundational phase (pre-2009)
- Subsection 3.5.2: Cyber Counterintelligence's emergence as an academic research theme (2009 -2012)
- Subsection 3.5.3 Cyber Counterintelligence crystallisation as a distinctive academic subdiscipline (2012 – present).

3.5.1 FOUNDATIONAL PHASE (PRE-2009)

As far as could be surmised from available literature, the explicit term 'cyber counterintelligence' first emerged in the US statutory security establishment during the early 2000s (see US 2004, French & Kim 2009). Prior to the 2000s, however, CCI was practiced in the statutory security establishment of the US and the security structures of some other countries. In this regard, French and Kim (2009) rightly assert that "cyber CI has existed *de facto* since the introduction of IT to intelligence, defence, and national security and has grown as FISs [Foreign Intelligence Services] have embraced cyber tradecraft."

Concurrent with CCI's *de facto* existence in statutory security circles, a few sporadic academic articles in the 1980 and 1990s expounded key CCI notions - although without using the actual term 'cyber counterintelligence'. Such notions included the advocating of an integrated CI approach, which not only has defensive and offensive missions, but also synchronises human and technical resources. The earliest peer-reviewed article found in consulted literature referring to such application of a CI approach to the IT realm is contained in the electronic library of the *Institute of Electrical and Electronics Engineers (I.E.E.E.)*. This item, authored by Stone and Tucker (1988), is entitled

‘Counterintelligence and Unified Technical Security Programs in Security Technology’. The authors expound effective CI as “unified multi-disciplinary concept” consisting of “proactive and defensive” missions. Stone and Tucker (1988) further argue that “advanced technology” is part of the multi-disciplinary CI entirety and thus serves both “proactive” (offensive) and defensive missions.

In a related further contribution in the *I.E.E.E.* library, Stone and Bluitt (1993) further expanded on the idea of executing “advanced technological countermeasures” as part of “a pervasive counterintelligence (CI) mandate.” Also Stone and Bluitt (1993) directed their paper specifically at the US statutory CI effort.

While both papers (Stone & Tucker 1988, Stone & Bluitt 1993) centre on rectifying perceived deficiencies in the US national CI endeavour thirty years ago, their key contentions on CI as “unified multi-disciplinary concept” of which “technological” measures are a part, hold relevance up to this day. Consequently, these early works have contextual and conceptual bearing on our **FCCI**’s design.

No articles or papers of direct CCI-relevance were found in consulted databases for the seven-year period 1994 – 2001. The mid-1990s did, however, see the emergence and exponential growth of literature in the field of **information warfare.** Such books, to name a few, include those by Molander, Riddle & Wilson (1996), Molander *et al.* (1998), Denning (1999), Kopp (2000), Hutchinson & Warren (2002), Jones, Kovacich & Luzwick (2002), Armistead (2004) as well as Hutchinson (2006). The launching of specialised conferences and journals (such as the *Journal of Information Warfare*) further attested to the growing prominence of information warfare (and later on to that of its subset cyber warfare). For the overwhelming part, works on information warfare make scant reference to counterintelligence and *vice versa*.

The first peer-reviewed article identified that specifically employs the term “cyber” in conjunction with “counterintelligence” appeared in a 2002 issue of the *Journal of Information Warfare*. As suggested by the title of their article ‘Dominating the attacker: Use of intelligence and counterintelligence in cyber warfare’, Davey and Armstrong (2002) examine Intelligence and CI's role in augmenting cyber warfare. Cyber warfare in turn, is firmly positioned as a subset of information warfare. By “employing intelligence and counterintelligence techniques that are superior to those of the attacker,” argue Davey and Armstrong (2002), the “cyber warfare defender” is more likely to prevail. Davy and Armstrong (2002) urge a more “aggressive” posture that includes deception. One such example cited, is allowing the “attacker [to] gain access

to information that is actually incorrect, thus providing incorrect intelligence." In respect of CCI's conceptual evolvement and especially CCI's relation to cyber warfare, the contribution of Davy and Armstrong (2002) represents a milestone and is – similar to those by Stone and Tucker (1988) and Stone and Bluitt (1993) - of contextual and conceptual importance to our **FCCI**'s design.

Our survey found no CCI-relevant publications for the next five years (2002-2008). Thus, in as far as consulted databases are concerned, CCI's foundational phase was characterised by a few sporadic academic contributions.

3.5.2 CYBER COUNTERINTELLIGENCE'S EMERGENCE AS A RESEARCH THEME (2009 - 2012)

Following a sporadic foundational phase, 2009 marked CCI's emergence as a specific research theme attracting growing interest. In that year, a seminal article appeared in the launch edition of the *National Intelligence Journal* (French & Kim 2009). This was the first academic publication (in consulted literature) to use the term "cyber counterintelligence." In this article, entitled 'Acknowledging the revolution: The urgent need for cyber counterintelligence', French and Kim (2009) call on the US intelligence community to move away from the notion that CCI is mostly part of "defensive Information Warfare." Instead, French and Kim (2009) urge the US to be more active and offensive in its approach to CCI. The work's relevance extends beyond the US context. French and Kim (2009) explicitly define CCI, explain CCI's missions within the context of CI, and offer various other insights on aspects useful to the further development within this field in general and our **FCCI** in particular. Such aspects include the role of CCI in information warfare, critical infrastructure protection as well as the CCI process and strategy.

No other peer-reviewed articles and papers were found in consulted literature for the 2009-2012 period. It must however be emphasised strongly that the absence of academic articles on CCI in consulted literature, belies CCI's emergence as a research theme two reasons. Firstly, there were several CCI contributions during this period in other literature categories (see Section 3.8 entitled 'Other literature') and in publications not covered by this article's selective review (see for example US Naval War College 2018, *Library Guidelines* on "Counterintelligence: Cyber Threat"). Secondly, the nature and extent of academic contributions on CCI from 2013 onward, strongly suggest that CCI attracted research interest in the preceding years (2009-2012). Phrased differently, research was done in the 2009-2012 but the fruits thereof, in

the main, only reflected from 2013 onward. The initiation of CCI research at the University of Johannesburg in 2012 serves as one such example (University of Johannesburg, 2018a).

3.5.3 CYBER COUNTERINTELLIGENCE CRYSTALLISATION AS AN ACADEMIC SUBDISCIPLINE (2013– present)

As from 2013, a consistent stream of peer-reviewed papers and articles signalled CCI's emergence as an academic subdiscipline. Indicative in this regard, the European Conference on Cyberwarfare and Security (ECCWS) in 2014, for the first time since its inception in 2001, featured a dedicated 'Cyber Intelligence – Cyber Counterintelligence' track. Internationally, significant contributions in English were made by researchers from the US, Australia, Sweden and South Africa.

3.5.3.1 Contributions from the United States

The bulk of academic contributions from the US stemmed from **Utica College**. Utica is a leading academic institution in the cybersecurity field and holds designations of academic excellence from the US National Security Agency, the US Department of Defense as well as the US Department of Homeland Security (Utica 2018). The college's Master of Science Cybersecurity programme offers CCI as a specialisation subject. This programme resulted in several "capstone project" papers (comparable to mini-dissertations in other countries) as well as a master's dissertation, with CCI as a specific focus (Knowles 2013, Black 2014, Fieber 2015, Putnam 2015, Justiniano 2017). Since these contributions flow from a master's programme, they are later discussed in more detail in Section 3.6 ('Master's and doctoral studies'). Suffice to state here that this Utica research constitutes indispensable contributions to CCI and our **FCCI** on the conceptual, theoretical and praxis levels.

Also in the USA, the concept of CCI has been attracting interest from researchers at the **Mitre Corporation**. The Mitre Corporation is a prominent US federally funded institution with an estimated revenue of $1.4 billion (Bloomberg 2018). It provides "systems engineering, research and development, and information technology support" to US government departments such as the Department of Defense and the Department of Homeland Security (Bloomberg 2018). Mitre's prioritised areas of research include cybersecurity, emerging and disruptive technologies, intelligence, surveillance, and reconnaissance" (Bloomberg 2018). In recent years, Mitre researchers have been pioneering work on denial and deception in cyber defence (Heckman *et al*. 2015). Branching out from their research on denial and deception, the "applications of cyber

counterintelligence" to "active cyber defense" was subsequently examined (Heckman *et al*. 2015; Stech & Heckman 2018). Flowing from this research Stech and Heckman (2018) contribute a book chapter, which is undoubtedly one of the most incisive and significant works on CCI to date. Its contribution to our **FCCI** is highlighted in Section 3.7 ('Books').

3.5.3.2 Contribution from Australia

Subsection 3.5.1 pointed out Davy and Armstrong's (2002) contribution as an important milestone in CCI's conceptual evolvement. As far as could be ascertained from consulted sources, CCI did not feature as a specialised theme within Australian academic circles before 2018. While Australian academics continued to make leading contributions to information warfare, also this literature for the most part made scant or no reference to counterintelligence more generally.

However, in 2018 Stech and Heckman's (2018) chapter was included in a book compiled under editorship of Australian academic Hank Prunckun. Prunckun is a leading academic authority in Intelligence Studies (notably on counterintelligence) and he is extensively cited in this thesis (Prunckun 2012, 2014, 2018). His book, further discussed in Section 3.7 of this thesis, hopefully signals growing academic interest in CCI also in Australian academic circles.

3.5.3.3 Contribution from Sweden

Albeit considerably more limited in scope than the research in the US, papers delivered at two *I.E.E.E.* endorsed conferences in 2013 reflected growing interest also outside the USA. In August 2013, at the *European Intelligence & Security Informatics Conference* in Sweden, Sigholm and Bang (2013) submitted a paper entitled 'Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats.' Moving from a statutory military perspective, the paper is primarily aimed to advance a "comprehensive process that bridges the gap between the various actors involved in CCI." Sigholm and Bang (2013) present this model to specifically configure the "offensive CCI attribution process." On closer scrutiny, this model does not actually deal with the whole "offensive CCI attribution process"; instead, it is limited to an all-source information flow and analysis architecture to be employed for attribution purpose. Nonetheless, Sigholm and Bang's (2013) work was informative to the CCI process we constructed as an **FCCI** building block (See Chapter 13).

3.5.3.4 Contributions from South Africa

On the heels of Sigholm and Bang in 2013, Duvenage and von Solms (2013) presented 'The case for cyber counterintelligence' at the I.E.E.E. endorsed *5th International Conference on Adaptive Science and Technology* hosted in South Africa. The paper defines key CCI concepts and advance conceptual constructs which explain CCI and its relation to CI. Duvenage and von Solms' (2013) paper formed part of a dedicated CCI research project initiated in 2012 at the University of Johannesburg's Cybersecurity Centre (UJCC) from which several other contributions would follow (University of Johannesburg 2018a). UJCC's website describes the project's aim as establishing CCI as a multi-disciplinary field of academic enquiry within the South African context (University of Johannesburg 2018a). To this end, the UJCC project pursues two complementary, yet parallel research streams, aimed respectively at:

1) Designing an overarching framework for conceptualising and explicating CCI as a distinctive academic field of enquiry, and;
2) developing a framework for a CCI maturity model for application by state and non-state actors within developing countries.

The **FCCI** advanced in this thesis is a direct outcome of the first research stream. Building on Duvenage and von Solms (2013), this research stream progressively advanced conceptual constructs to academically explain what CCI is, how it works and how it dovetails with other academic disciplines and theory. Such notional constructs, include a CCI-posture matrix model, CCI process model as well as a taxonomy of CCI tactics, tools, techniques and procedures (TTTPs). These notional constructs were submitted per the following peer-reviewed papers and a journal article:

- Duvenage and von Solms (2014) 'Putting counterintelligence in cyber counterintelligence' in the *Proceedings of the 13th European Conference on Cyber Warfare and Security,* Piraeus, Greece.
- Duvenage and von Solms (2015) 'Cyber counterintelligence: Back to the future' in the *Journal of Information Warfare*.
- Duvenage, von Solms and Corregedor (2015) 'The cyber counterintelligence process – a conceptual overview and theoretical proposition' in the *Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, United Kingdom.
- Duvenage, Jaquire and von Solms (2016) 'Conceptualising cyber counterintelligence – two tentative building blocks' in the *Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, Germany.

The above mentioned works developed constituent parts of an **FCCI**, but did not as yet advances an overarching **FCCI**. In 2017, these works were synthesised with the forwarding of an overarching **FCCI** in a paper entitled 'A conceptual framework for cyber counterintelligence – theory that really matters' (Duvenage, Sithole & von Solms 2017). This paper subjected this thesis's core contentions for peer review to the *16th European Conference on Cyber Warfare and Security* (See Annexure F). The positive feedback from the peer-review process described the paper, and by extension the thesis, as laying the foundations for a structured CCI approach.

UJCC's second research stream, to recapitulate, aims to develop a CCI maturity model with emphasis on governments and non-state actors in emerging countries (University of Johannesburg 2018a). The research stream adapted central elements of our **FCCI**, for application to a CCI maturity model (Jaquire 2018). Peer-reviewed papers on a framework for a CCI maturity model which affirms the utility of our **FCCI** are as follow:

- Jaquire and von Solms (2017a) 'Towards a cyber counterintelligence maturity model' in the *Proceedings of the 12th International Conference on Cyber Warfare and Security*, Wright State University, Air Force Institute of Technology, Dayton (US).
- Jaquire and von Solms (2017b) 'Developing a cyber counterintelligence maturity model for developing countries' in the *Proceedings of the 2017 IST–Africa Conference*, Windhoek, Namibia.
- Jaquire and von Solms (2017c) 'Cultivating a cyber counterintelligence maturity model' *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland.
- Jaquire, V.J., Duvenage, P.C. & von Solms, S.H. (2018) 'Building the CCI dream team' in the *Proceedings of the 17th European Conference on Cyber Warfare and Security*, Oslo, Norway, June.

3.5.3.5 Contributions from other countries

As was observed in Section 3.3, we did not cover or purposefully review literature in other languages. Nonetheless, we noted notifications of citations of our research (e.g. Duvenage & von Solms 2014, Duvenage & von Solms 2015) in some other languages. These citations not only point to a wider academic interest in CI but also suggest the utility of our **FCCI**. Two such examples are citations of our **FCCI** research in the following articles featured in publications linked to the state security structures of respectively Italy and the Peoples' Republic of China (PRC):

- Huang，Z (2015) 分析了网络反情报的形成和发展的背景，总结归纳了网络反情报的对抗性，技术性和隐蔽性特点. 提出在现代网络安全威胁形势下. 网络反情报具有保护网络重要信息，打击网络恐怖主义等非法 活动，掌控敌对方网络情报活动等作用. 认为将网络反情报的理论和技术引入情报体制和工作 ['Background, Characteristics and Significance of Cyber Counterintelligence'] in *Information Research*, Issue 12, People's Public Security University of China.
- Teti, A (2016) 'Cyber counterintelligence – Il controspionaggio nel cyberspazio' ['Cyber Counterintelligence – counterespionage in cyberspace'] *Gnosis - Italian Intelligence Magazine*, Information and Internal Security Agency, 4 (16).

In this section, we examined CCI's academic evolvement at the hand of an overview of peer-reviewed articles and papers. Specific reference was made to the pertinence of this research to our **FCCI**'s design. In the next section, master's and doctoral research focused on CCI are explored.

3.6 MASTER'S AND DOCTORAL STUDIES

The search term 'cyber counterintelligence' (and variations thereof) showed numerous master's and doctoral studies of possible relevance to a CCI literature review. On closer analysis, however, most of these studies do not have CCI as a primary focus and CCI is not explored in depth. Instead, CCI is cursorily referred to as part of the broader statutory CI mandate and mostly addressed within challenges faced by the US Intelligence community. Ferguson's (2012) thesis entitled *Increasing the effectiveness of U.S. counterintelligence: Domestic and international micro-restructuring initiatives to mitigate cyber espionage* serves as one such example. For the reasons mentioned, studies such as this do not contain elements directly applicable to the construction of our **FCCI**.

3.6.1 MASTER'S RESEARCH AT UTICA COLLEGE

Bucking this trend, master's studies completed at Utica College from 2013 onwards delivered contributions that are pioneering and invaluable in respect of CCI's academic crystallisation and evolvement. While conducted within the context of US national interests and security, these studies have application and academic relevance much wider than the US. On the whole, important contributions are made to explicating CCI on the conceptual, theoretical and praxis levels. Consequently, these studies were also highly informative and useful to our **FCCI**'s design. The following are some examples:

- In his research entitled *Applying computer network operations for offensive counterintelligence efforts*, Knowles (2013) identifies key aspects of Computer Network Operations (CNO). These aspects are then aligned with the broader intelligence and CI processes. In so doing “counterintelligence skills and techniques” are leveraged to “assimilate cyber activities” into an organisation’s Intelligence endeavour.
- Boawn's (2014) capstone paper entitled *Cyber counterintelligence, defending the United States' information technology and communications critical infrastructure from Chinese threats* argues for offensive CCI featuring more centrally in the US intelligence community's defences "against Chinese cyber aggression" targeting the US' "critical infrastructure and key resources" (Boawn 2014). The study’s definitions of CCI-related concepts and his description of CCI execution draw on existing research. Boawn (2014) does not set out to and does not offer an overarching schema which explains CCI. Neither does he advance novel CCI constructs. Nonetheless, his research offers insights on CCI's role in critical information technology and communications infrastructure more generally.
- Effective CCI, argues Black (2014), is multidisciplinary and involves unique skill sets. In his thesis, entitled *The complexity of cyber counterintelligence training*, Black (2014) proceeds with identifying the implications thereof for CCI training. Black then advances two useful notional constructs namely (1) a CCI training model and (2) a CCI training proficiency path.
- As suggested by the research title, Putnam’s (2015) *Digital mirrors casting cyber shadows - the confluence of cyber technology, psychology, and counterintelligence* emphasises CCI’s multidisciplinary nature. Putnam (2015) points out that a successful CI (and thus CCI) programme should consider the opportunities that technology presents as well as certain psychological “principles of persuasions” and motivation. The study details some offensive and defensive CCI applications of these opportunities and principles. Emphasis is placed in this regard on optimising the CCI targeting and the recruitment processes.
- The interplay between practice and theory which characterises Utica College’s research is reflected in Fieber’s (2015) commendable contribution *The Iranian computer network operations threat to U.S. critical infrastructures.* Fieber (2015) analyses “the Iranian computer network operations (CNO) threat to U.S. critical infrastructures” and proceeds with recommending defensive measures to

mitigate this threat. The paper culminates in a handy proposition on a phased, CCI process model "designed to mitigate conditions favorable to the attacker and restore the advantage to the organizational defenders" (Fieber 2015)

- In a further outstanding contribution, Justiniano (2017), with the research title *Advancing the capacity of a theatre special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone,* examines CCI's role in the US military milieu with a focus on the hybrid threats posed by Russia and the role of CCI in mitigating and engaging this threat. Justiniano's (2017) research is indispensable reading for examining CCI's role in hybrid warfare more generally. The study identifies critical CCI roles and skillsets before proceeding to propositions on integrating CCI with the US "Cyber Mission Assurance (C-MA)" process in a manner supportive of "Theater Special Operations Command (TSOC)."

As reflected from the preceding review and as will be seen in subsequent chapters, Utica's research offers useful insights, and in some instances contributions, to our **FCCI**, on the conceptual, theoretical and praxis levels. Utica's research include propositions on conceptual frameworks and models that explain aspects of CCI - such as CCI training (Black 2014), the CCI process (Fieber 2015) and various constructs for optimising CCI in countering hybrid warfare (Justiniano 2017).

Unlike our **FCCI**, these studies do not advance an overarching conceptual framework which structure's and expounds CCI as a distinctive subdiscipline.

3.6.2 DOCTORAL RESEARCH AT THE UNIVERSITY OF JOHANNESBURG

In a similar vein, Jaquire's (2018) a doctoral thesis completed at the University of Johannesburg is specifically focused on a specific aspect of CCI, namely *A framework for a cyber counterintelligence maturity model*. Like the preceding papers (Jaquire & von Solms 2017a-c), the thesis adapts central elements of our **FCCI** for constructing the maturity framework.

The preceding two sections (Section 3.5 and Section 3.6) focused on academic, peer-reviewed literature which range from papers and articles to master's and doctoral studies. In next section, we assess books published on CCI.

3.7 BOOKS

The past two decades has seen an exponential rise in the number of books from reputable publishers dealing with information warfare (see Section 3.5.1) and cybersecurity. However, until very recently, even outstanding books that address aspects of high relevance to CCI make scant reference to CI and CCI. One such example is Heckman *et al*.'s (2015) *Cyber denial, deception and counter deception – A framework for supporting active cyber defense*. Despite this work arguably setting the standard for future works on cyber denial and deception in general, only four sentences in the entire book mentions the term 'counterintelligence' and there is no mention of 'cyber counterintelligence'.

The first book identified by the survey conducted for this thesis, which has a significant CCI focus, was published in 2012 with the title *Reverse deception – Organized cyber threat counter-exploitation* (Bodmer *et al.* 2012). Pitched as practicable guide for "IT security professionals", Bodmer *et al.*'s (2012) work is highly significant also from an academic perspective. The book comprehensively examines the role of CCI in countering cyber threats through the engagement of hostile actors. In addition to CCI tactics, techniques and procedures (TTPs), the authors also explore CCI on a conceptual level. This includes postulations on CI missions was well as CCI's interface with CI and other Intelligence fields. In nutshell, Bodmer *et al.* (2012) is essential reading for any researcher interested in CCI. It is also extensively used and referenced in the design of our **FCCI** throughout the thesis.

At least in as consulted literature is concerned, the next book to include a pertinent and significant CCI focus was under the editorship of Prunckun (2018) and entitled *Cyber Weaponry Issues and Implications of Digital Arms*. While the book has several chapters useful to CCI, Chapter Two is pertinently dedicated to CCI. Under the title, 'Human Nature and Cyber Weaponry: Use of Denial and Deception in Cyber Counterintelligence', Stech and Heckman (2018) advance a masterful contribution which anyone serious about CCI has to consult. Stech and Heckman (2018) primarily aim to advance a "cyber counterintelligence framework in active cyber defences". This system is "referred to as the cyber deception chain, to mitigate cyber spy actions within the cyber espionage 'kill chain' " (Stech & Heckman 2018). To lay a foundation for their CCI framework, Stech and Heckman 2018) explain the need for CCI. They proceed with appraising CI definitions, status and existing frameworks with a view on application to active defense in CCI. Stech and Heckman (2018) furthermore observe the existing

body of CCI academic research. Proceeding from this basis, they present a CCI framework for “active cyber defense” (Stech & Heckman 2018). Stech and Heckman (2018) extensively cite, and incorporate notions advanced in, our **FCCI** research (Duvenage & von Solms 2014; Duvenage, von Solms & Corregedor 2015; Duvenage, Jaquire & von Solms 2016). A building block of our **FCCI**, namely the CCI Matrix (see Chapter 10, Section 10.4) is at the core of Stech and Heckman’s (2018) framework. Their work demonstrates the matrix's application by means a hypothetical case involving North Atlantic Treaty Organisation (NATO) and the Russian Federation (Stech & Heckman 2018). Although published during the finalisation phase of our **FCCI** research, Stech and Heckman’s (2018) work nonetheless added considerable value to this thesis. (Please see Chapter 10 for more detail).

This section evaluated salient books pertinent to CCI and our **FCCI**'s design. We now proceed with evaluating other literature forms.

3.8 OTHER LITERATURE

Especially during the past eight years, there has been an upsurge in literature dealing with “threat intelligence,” “cyber intelligence” and “cyber threat intelligence”. Cybersecurity vendors, which are increasingly modelling their products and services on concepts, derived from the state security and intelligence realms in part fuel this upsurge. In contrast to the bourgeoning discourse on for example 'threat intelligence' and 'cyber intelligence', contributions to CCI are more limited but growing. In the main, contributions offer high-level explanations of what CCI is and point to the advantages that CCI practices could have in proactively addressing cyber insecurity. While ‘commercial’, such works nonetheless contribute to explicating CCI in concrete terms and, in some instances, are consequently also of academic value. In this regard, works by Bardin (2011), Farchi (2012) and Lee (2014) can be singled out.

The following examples of article headlines give a sense of the nature of contributions in commercial online literature:

- ‘Cyber counter intelligence’, in *Defense Tech Magazine* (Carrol 2009).
- ‘Ten commandments of cyber counterintelligence’ by Bardin (2011), first featured on the IDG News Service's online platform *CSO Online*.
- ‘Offensive counter-intelligence and cyberwarfare – A paradigm shift in information security’ on the *Information System Control and Audit Association (ISACA)* website (Farchi 2012).

- ‘To thwart hackers, firms salting their servers with fake data’, in *The Washington Post* (Nakashima 2013)
- ‘Cyber counter-intelligence makes a difference’, featured on the South African ITWeb website (von Solms 2014).
- ‘Cyber counterintelligence: From theory to practice’ by Lee (2014), first published on the website of the cybersecurity vendor *Tripwire*.
- ‘Shifting paradigms: The case for cyber counter-intelligence’, in *InformationWeek* (Firestone 2015).
- ‘Counter-intelligence techniques may help firms protect themselves against cyber-attacks’, published in *The Economist* (2015).

In our construction of the **FCCI**, we found CCI literature, such as those cited above, to be useful in delineating key concepts and principles but less pertinent to the actual design of our overarching **FCCI**.

This section reviewed some examples of other literature on CCI. In section to follow, the article concludes with findings and observations on the way forward.

3.9 SUMMARY AND CONCLUSION

This chapter was aimed at providing an overview and evaluating existing literature on CCI. We found that, apart from a paper directly flowing leading up to this thesis (Duvenage, Sithole & von Solms 2017), no overarching conceptual FCCI exists in the surveyed literature. Consequently, we validated the thesis’s problem statement and the objective to construct such an FCCI. The evaluative literature review we advanced is also central to this thesis’s inductive qualitative methodology and its academic credibility (See Chapter 1, Section 1.4 and Chapter 2, Section 2.2).

It is clear from the literature review that our research leading up to the FCCI constitutes a significant contribution to the field.[3] Furthermore, since we followed a structured approach to the literature review, a 'scaffold' has been established to which further research on CCI as an emerging academic field can be added. The review’s usefulness in this regard was confirmed by the successful peer-review and presentation thereof at the *17th European Conference on Cyber Warfare and Security* with the tile ‘A selective

[3] This assertion is substantiated in more detail in Chapter 13 (Subsection 13.6.5).

literature review on cyber counterintelligence' (Duvenage, Jaquire & von Solms (2018a). Subsequently, an expanded version was published per invitation in the *Journal for Information Warfare* with the title 'Towards a literature review on cyber counterintelligence' (Duvenage, Jaquire & von Solms 2018b).

The literature review concludes Part 1 of the thesis during which the foundation was laid for the FCCI's construction. In the next chapters (Chapters 4–13), we present the FCCI and its eight notional building blocks.

PART 2

HIGH-LEVEL OVERVIEW OF THE CONCEPTUAL FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

Part 2 presents a high-level overview of our integrated FCCI. By means of graphics and narratives, the FCCI's eight building blocks and the synergy between these blocks are shown. The integrated FCCI is the 'blueprint' of the rest of the thesis. As supplement to the ‘blueprint’, the design logic we present concisely explains the reasoning behind the FCCI's block-by-block construction. This design logic is a cursory step-by-step 'construction manual' to guide the reader. Part 2 consists of **Chapter 4**.

CHAPTER 4

OVERVIEW OF THE INTEGRATED FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

4.1 INTRODUCTION

In the first part of this thesis (Chapters 1–3), we laid the foundation for presenting our FCCI. This second part of the thesis (Chapter 4) contains:

(1) a high-level overview of our integrated FCCI, and
(2) the condensed logic for constructing our FCCI block by block in the chapters to follow (i.e. Chapters 5–13)

In the **high-level overview**, we synergistically combine the FCCI's building blocks into an integrated FCCI. Our integrated FCCI is, to use an analogy, the **blueprint** for the end product of this thesis's 'assembly line'. This high-level overview of the integrated FCCI thus gives the reader a preview of the study's final destination.

The condensed **logic**, to extend the analogy, is a bird's eye view of the main points of the **assembly line** for constructing our FCCI. The condensed logic is thus the narrative explicated step-by-step 'manual' which explains to the reader (in broad terms) how we will arrive at the final destination.

Being the study's 'manual', the reader can thus refer back to this chapter for clarity in reading subsequent chapters (Chapters 5–13). This chapter draws on, and contains verbatim extracts from, the peer-reviewed paper by Duvenage, Sithole & von Solms (2017), which is attached to this thesis as **Annexure F**.

The rest of the chapter is structured as follows:

- Section 4.2: Overview of the integrated framework for cyber counterintelligence
- Section 4.3: Sequential design logic of the framework for cyber counterintelligence
- Section 4.4: Conclusion

4.2 OVERVIEW OF THE INTEGRATED FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

In Chapter 1 (Section 1.5) and Chapter 2 (Section 2.3), we referred to the eight building blocks of our FCCI. We mentioned that each of these building blocks is essential to explain different dimensions of effective CCI. Viewed separately and on their own, each building block can however explain fully *neither* CCI's respective dimensions *nor* CCI as a whole. The explanatory power of the FCCI as an academic construct, as well as its usefulness in CCI practice, lies in the synergy between its eight building blocks. In this case, the whole (integrated FCCI) is indeed more than the sum of its parts (building blocks).

This integrated synergy can graphically be presented as follows:

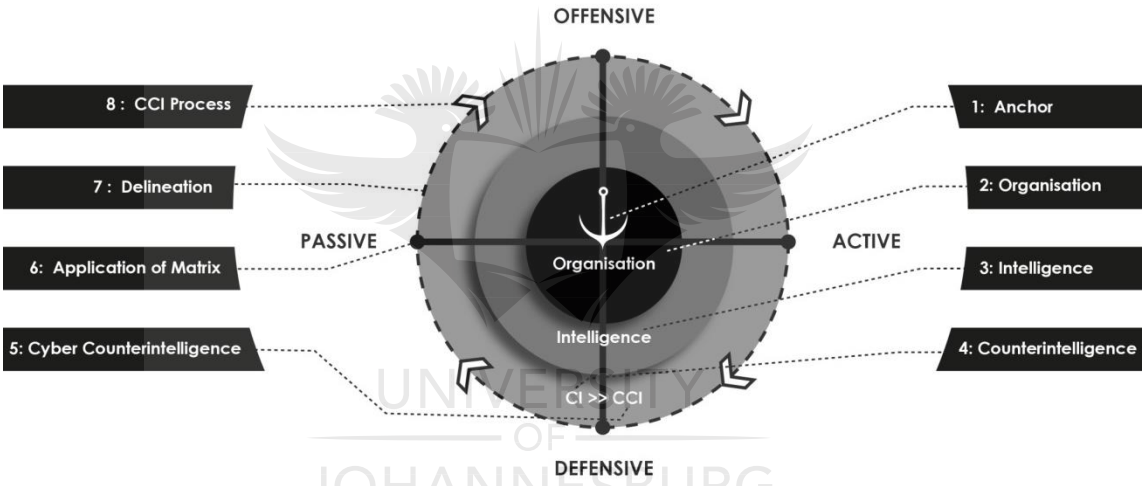


Figure 4: Integrated FCCI (Duvenage, Sithole & von Solms 2017)

In this section, we emphasised the importance of synergistically integrating the various CCI building blocks. We then graphically depicted the integrated FCCI to serve as a 'blueprint' and preview of the thesis's 'destination'. In the next section, we provide the condensed logic behind the FCCI's block-by-block construction.

4.3 SEQUENTIAL DESIGN LOGIC OF THE FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

Whereas we integrated the CCI's building blocks in Section 4.2, a cursory explanation of the logic of the FCCI require us to 'deconstruct' Figure 4 and then 'reassemble' the FFCI block by block. To explain the logic, broad reference is made to the substance of

each building block. Inevitably, this results in some duplication in Chapters 5 to 13. Likewise, graphical depictions of the addition of FCCI building blocks in this chapter (Figures 5–13) are repeated in subsequent chapters (5–13).

Since this chapter is intended to guide the reader through the rest of the thesis, we link the building blocks with the specific chapters devoted to their detailed discussion. This is done by stipulating the **applicable chapter in brackets** for each heading, for example:

4.3.1 Building Block 1: Theoretical Anchor (**Chapter 5**)

In this subsection, we explicated our approach to discussing the FCCI's sequential design logic. We now proceed with the block-by-block assembly and explanation of the sequential logic of our FCCI.

4.3.1 BUILDING BLOCK 1: THEORETICAL ANCHOR (CHAPTER 5)

In Chapter 5, we start by **anchoring** our FCCI in **theory**. This is necessary since an academic credible FCCI has to be anchored in and build upon existing theory (see Section 2.2 of Chapter 2). This theoretical anchoring is therefore the FCCI's first building block. **Building Block 1** positions the FCCI as part of the existing theoretical discourse and advances the core theoretical contentions on which we base the FCCI's subsequent building blocks. Graphically, the FCCI's theoretical anchor can be depicted as follows:

Figure 5: Building Block 1 – Theoretical Anchor (Duvenage, Sithole & von Solms 2017)

4.3.2 BUILDING BLOCK 2: ORGANISATION (CHAPTER 6)

CCI ultimately exists because of, and has to be configured in accordance with, the interests of the 'organisation' it serves. This generic concept of an organisation refers to various types of entities, ranging from nation states and multinational corporates to smaller businesses and non-governmental organisations (NGOs). Since it is CCI's

raison d'être, the **organisation** is **Building Block 2** of our FCCI and is discussed in Chapter 6. Graphically, we can depict the addition of this building block as follows:

Figure 6: Building Block 2 –Organisation (Duvenage, Sithole & von Solms 2017)

4.3.3 BUILDING BLOCK 3: INTELLIGENCE (CHAPTER 7)

While it is an indispensable instrument, CCI cannot secure and pursue an organisation's interests all by and for itself. It has to be done as part of an organisation's intelligence endeavour. By way of analogy, CCI is but one 'tool type' within an organisation's intelligence 'toolkit'. Therefore, **intelligence** is advanced and discussed in Chapter 7 as **Building Block 3** of our FCCI. The addition of intelligence as a building block can graphically be illustrated as follows:

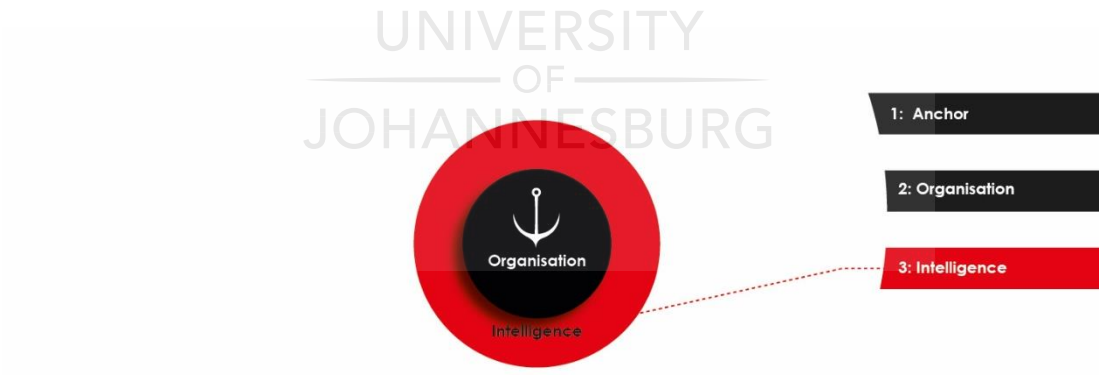


Figure 7: Building Block 3 – Intelligence (Duvenage, Sithole & von Solms 2017)

In Chapter 7, we show CCI to be interlinked with all three primary elements of intelligence, namely: (1) positive intelligence, (2) CI and (3) covert action.

4.3.4 BUILDING BLOCK 4: COUNTERINTELLIGENCE (CHAPTER 8)

Although it is indeed interlinked with all three primary elements of intelligence, CCI is per definition and in practice a subset of CI. By way of analogy, CCI is one of the 'tool types' within the CI 'toolset'. Practically and conceptually, CCI is thus interwoven with the whole of the multidisciplinary CI effort. In other words, CCI is not a neat compartment within CI; it involves, and requires the clarity of all the other CI fields. Consequently, **CI** constitutes **Building Block 4** of the FCCI. Given its importance to our FCCI, this building block is one of the building blocks most comprehensively discussed in this thesis (Chapter 8). This includes outlining a four-sector CI matrix consisting of offensive–defensive and passive–active axes. The CI matrix is explained in this chapter with a view to its application to CCI per Building Block 6 later on (in Chapters 11 and 12). Graphically, the addition of CI as the FCCI's fourth building block can be depicted as follows:

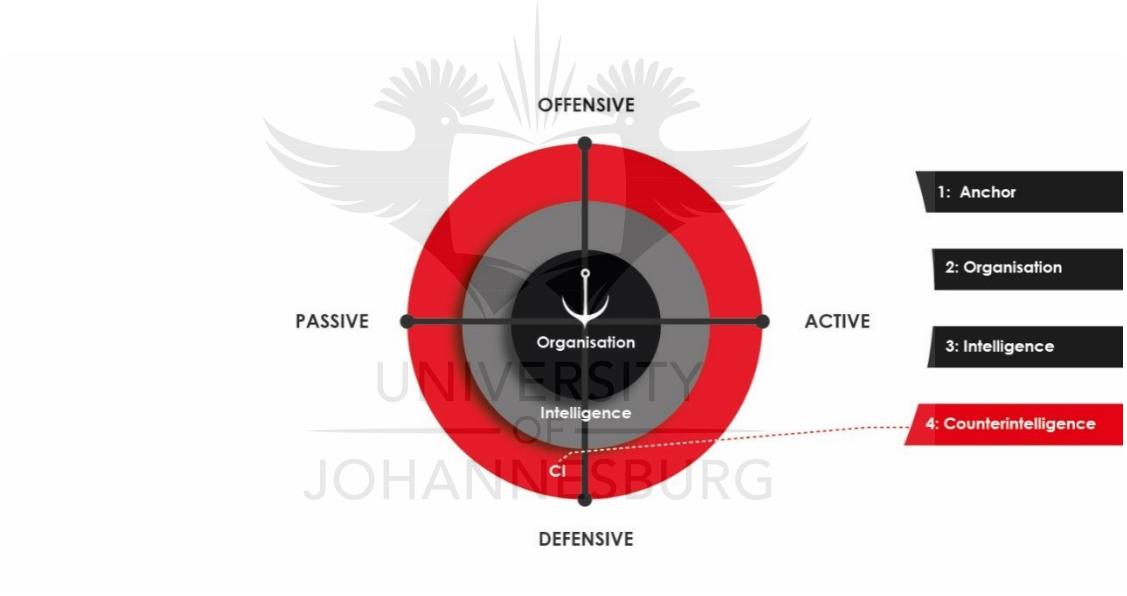


Figure 8: Building Block 4 – CI (Duvenage, Sithole & von Solms 2017)

4.3.5 BUILDING BLOCK 5: CYBER COUNTERINTELLIGENCE (CHAPTER 9)

While firmly dovetailed with multidisciplinary CI, **CCI is above all a technical tool type**. The **CCI tool type**, which we advance as **Building Block 5** of our FCCI, comprises an extensive range of tools (technologies, measures and techniques). Most of these tools are not unique to CCI. What is unique is the application thereof in combination with other CI tools and in a manner best achieving CI's defensive and offensive missions. The addition of this building block can be illustrated as follows:

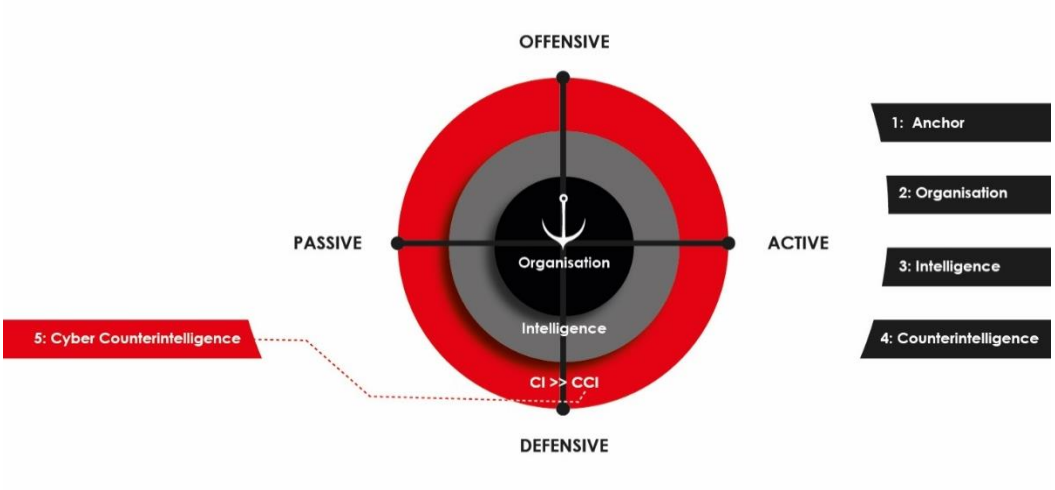


Figure 9: Building Block 5 – CCI (Duvenage, Sithole & von Solms 2017)

4.3.6 BUILDING BLOCK 6: CYBER COUNTERINTELLIGENCE MATRIX (CHAPTER 10 AND CHAPTER 11)

In Subsection 4.3.5 (Building Block 5), we noted that CCI tools can be deployed in offensive and defensive modes. A significant part of these tools can also be deployed in a passive and active mode. Optimally, CCI requires the employment of tools in all of the said modes. Effective CCI furthermore requires synergetic execution on the technical-tactical, operational and strategic levels.

To conceptually aid this complex task we add the following four-quadrant, three-tiered matrix as Building Block 6 of our FCCI:

Figure 10: CCI Matrix (Author)

As depicted in Figure 10, the matrix's horizontal plane, explains CCI's passive-defensive and active-offensive modes. This horizontal plane is discussed in Chapter 10. Chapter 11 proceeds with explaining the three-levels on which CCI functions as the matrix's vertical plane.

Graphically, the addition of the matrix to our FCCI looks like this:

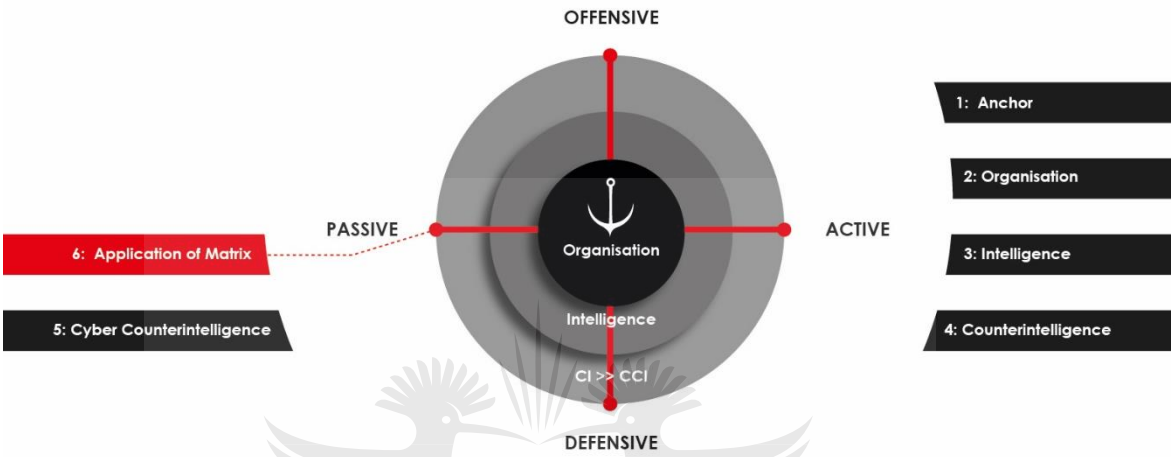


Figure 11: Building Block 6 – Application of the CCI Matrix (Duvenage, Sithole & von Solms 2017)

4.3.7 BUILDING BLOCK 7: DELINEATION (CHAPTER 12)

Even with all the previous building blocks in place, an organisation would seldom be able or legally allowed to execute the entire CCI endeavour on its own. Even nation states have to cooperate with non-state actors to achieve national goals. Consequently, effective CCI requires cooperation with other actors and delineating respective roles. Delineation is also important in the academic context. Treating CCI as a too wide and encompassing field will result in loss of focus. Simultaneously, CCI must be clear in terms of its relation with various other academic subjects and the areas of multidisciplinary research.

We can illustrate the addition of delineation and cooperation as the next building block of the FCCI as follows:

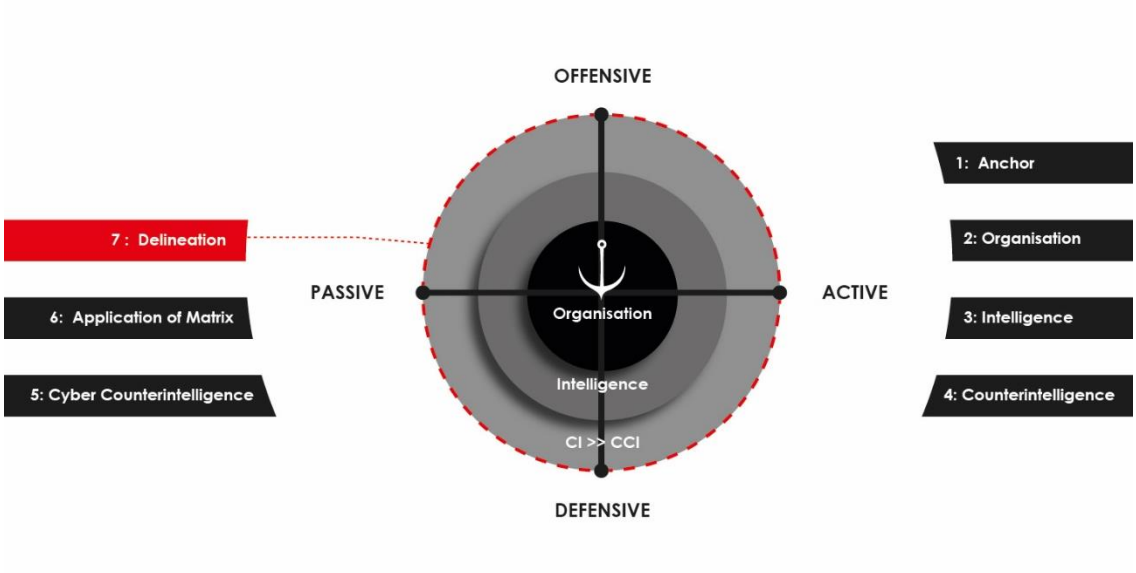


Figure 12: Building Block 7 – Delineation (Duvenage, Sithole & von Solms 2017)

4.3.8 BUILDING BLOCK 8: CCI PROCESS (CHAPTER 13)

The foregoing building blocks provide nearly all of the 'parts' necessary to academically explain and practically execute CCI. However, at this juncture, these parts – and thus the FCCI – are still 'static'. They lack the dynamism that synergistically combines and drives these different parts as an integrated process. Consequently, a CCI process model is proposed as the last building block of the FCCI. The addition of the CCI process as the eighth and last building block of our FCCI can be depicted as follows:

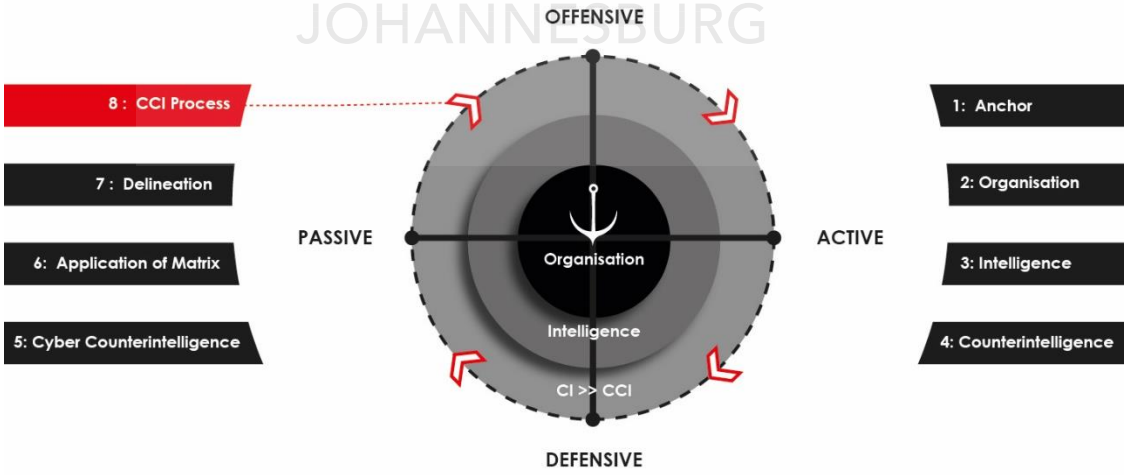


Figure 13: Building Block 8 – CCI Process (Duvenage, Sithole & von Solms 2017)

4.4 CONCLUSION

Whereas we integrated the CCI's building blocks in Section 4.2, a cursory explanation of the logic of the FCCI required as to 'de-construct' the integrated FCCI and the explain the building blocks.

In Part 2 of the thesis, which comprises Chapter 4, we thus presented the integrated FCCI and then briefly explained the logic behind its eight building blocks. This is intended to serve as a guide to the reader for the purpose of the more detailed explication of the FCCI’s building blocks in Part 3 of this thesis.

PART 3

EXPLICATION OF THE BUILDING BLOCKS OF THE FRAMEWORK FOR CYBER COUNTERINTELLIGENCE

In Part 3, we discuss the eight building blocks of our FCCI and sequentially construct the framework. The building blocks advanced in these chapters, which respectively and collectively explain what CCI is and how it works, are as follows:

- Chapter 5 - Building Block 1: Theoretical anchor
- Chapter 6 - Building Block 2: Organisation
- Chapter 7 - Building Block 3: Intelligence
- Chapter 8 - Building Block 4: Counterintelligence
- Chapter 9 - Building Block 5: Cyber Counterintelligence
- Chapter 10 - Building Block 6.1: Cyber Counterintelligence Matrix – Horizontal plane.
- Chapter 11 - Building Block 6.2: Cyber Counterintelligence Matrix – Vertical plane.
- Chapter 12 - Building Block 7: Delineation
- Chapter 13 - Building Block 8: Cyber Counterintelligence Process

CHAPTER 5

BUILDING BLOCK 1 – THEORETICAL ANCHOR

5.1 INTRODUCTION

Part 2 (Chapter 4) provided an overview of the integrated FCCI. In Part 3, which consist of Chapter 5 – 13, we proceed with discussing each of the FCCI's respective building blocks.

Throughout the thesis thus far, we emphasised the fact that our FCCI is a theoretical construct. Without negating CCI's multidisciplinary nature, we contended that the FCCI has its primary taproot within Intelligence Studies theory (see for example Section 1.1 of Chapter 1 and Section 2.2 of Chapter 2). In this chapter, we position FCCI within the context of Intelligence Studies theory by means of the following sections:

- Section 5.2: Theoretical anchor – Why it is needed and important as a building block
- Section 5.3: Challenges in designing a theoretical anchor as a building block
- Section 5.4: Qualifications for and approach to designing the building block
- Section 5.5: Explicating a theoretical anchor as the first building block
- Section 5.6: Conclusion

Graphically represented, the positioning of a theoretical anchor as the FCCI's first building block is as follows:

Figure 14: Building Block 1 – Theoretical Anchor (Duvenage, Sithole & von Solms, 2017)

5.2 THEORETICAL ANCHOR – WHY IT IS NEEDED AND IMPORTANT AS A BUILDING BLOCK

A theoretical anchor is needed and important for two interrelated sets of reasons, namely:

(1) Academic reasons, and
(2) Practical imperatives

5.2.1 ACADEMIC REASONS

The theoretical anchoring of our FCCI is necessary because it is required by academic exactitude and sound methodology. As a theoretical construct, our FCCI cannot be a loose-standing, theoretical island. In line with the requirements discussed in Chapter 2, our FCCI should coherently make clear what CCI is and how it works. To be coherent, logical and academically credible, this begins with fundamental notions of intelligence theory. Intelligence theory is overlaid on international relations theory in general, and the concept of 'national security' specifically. This means that our FCCI should reflect such thinking. Moreover, cognisance of long-established "international relationship scholarship" notions will aid us not only in design the FCCI, but also in properly understanding and appraising contemporary cybersecurity issues (Buchanan 2016).

Clearly then, to be academically credible, the FCCI has to duly consider and position itself as part of the existing theoretical discourse. Such anchoring provides a nexus for linking CCI with other academic fields and discourses. Properly designed, Building Block 1 acts as the central notional node that binds all further FCCI theory. It is the anchor to which we can constantly refer back when designing further FCCI building blocks.

5.2.2 PRACTICAL IMPERATIVES

The anchoring of our FCCI in theory is also important from a practical point of view. Theory is often regarded as abstract thinking that has little bearing on, or use in, the ‘real world’. Theory may even be deemed to be the opposite of practice. This is of course not the case – theory is highly relevant to practice and practice ought to inform theory. In the words of Lewin (as cited in Greenwald 2012): "There is nothing so practical as a good theory." This is especially the case for a complex field such as intelligence, and thus CCI (see Chapter 7 for the link between intelligence and CCI).

Commenting on the importance of theory, Betts (2004) asserts “intelligence failures” to be, for a significant part, the “result of bad theory”. Within CCI, the price of poor theory will ultimately be paid through more costly failures and damaging breaches. Theoretical constructs are thus clearly not ‘nice to have’ academic ‘toys’. These constructs, which include frameworks and models, condition our thinking and our approach to practice. To summarise, effective CCI practice presupposes a sound theoretical foundation. Our FCCI is precisely an attempt to establish such a foundation by linking CCI with existing intelligence theory. To this end, the chapter draws on earlier peer-reviewed CI research by the author (Duvenage & Hough 2011 and Duvenage 2011).

In this section, we highlighted the academic and practical imperatives of having a theoretical anchor as the first building block of our FCCI. In the next section, we highlight challenges in designing a theoretical anchor as an FCCI building block.

5.3 CHALLENGES IN DESIGNING A THEORETICAL ANCHOR AS A BUILDING BLOCK

Firstly, and contrary to what might be expected, **Intelligence Studies** is a relatively new discipline and is critically **under-theorised** (Johnson 2007). Moreover, in Chapter 1 (Section 1.1), we noted this theoretical paucity to be even more acute in relation to CI and CCI. For reasons noted (in Subsection 5.2.1), Intelligence – and thus ultimately our FCCI – cannot be discussed without reference to theoretical thinking within Intelligence Studies' mother discipline of Political Science and notably the specialisation field (within Political Science) of International Relations.

Our second challenge is that **neither International Relations nor Intelligence theory** is a **homogenous body of thought**. Not only are there various levels of theory, but the discourse is one of opposing meta-paradigms, multiple competing schools of thought and highly contested definitions.

On a meta-paradigmatic level, for example, positivists ontologically and epistemically hold reality as existing objectively from the scholar. The latter can therefore de-link himself/herself and conduct analysis that reflects the “real world” (van den Berg 2018; Du Plessis, 2001). Post-positivists assume a directly opposing position. Epistemologically and ontologically, the researcher cannot be de-linked from and pronounce an objective reality (Sterling-Folker 2006).

Moving from these two meta-paradigms (and hybrids thereof), a wide-array of schools of thought exist within International Relations theory. These include, to name but a few, realism, liberalism, constructivism, radicalism and post-structuralism. Moreover, within each of these schools, there are several streams of thinking. Within realism, classic and neo-realism are examples of such streams. Neo-realism, in turn, comprises proponents of offensive neo-realism and defensive neo-realism (Lomans 2017). Within the confines of our FCCI, these different schools of thought (and their respective streams) cannot be discussed in detail. These two challenges shaped our approach, which is discussed in the next section.

5.4 QUALIFICATIONS FOR AND APPROACH TO DESIGNING THE BUILDING BLOCK

To meet the said challenges, we have opted to assume a theoretical position (neo-realism) which in our view best explains intelligence, CI and thus ultimately our FCCI. We do so with four qualifications.

Firstly, we assume a **'generic' neo-realist position** without weighing the merits of other schools of thought or reflecting the different neo-realists streams. This does not imply a dogmatic conformation to all the core contentions of neo-realism or negation of the insight other schools may render if applied to CCI.

Secondly, we are duly cognisant of the fact that realist theorists "generally do not place non-state actors at the center of their theoretical propositions." (Laksman 2013) Realism is (in respect of international relations) focused on the nation state, while this study is aimed at presenting the FCCI as a general framework to also guide the CCI endeavours of other **types of entities and actors** (henceforth referred to as the **organisation**). In a similar vein, and within the context of this thesis, actors in opposition to the own organisation can include diverse state actors, non-state actors (e.g. business, criminal and activist entities) and even individuals.

Cognisance is taken of the fact that, at least normatively, an organisation other than nation states (or collectives thereof such as the North Atlantic Treaty Organisation [NATO]) is not supposed to exercise some intrusive, disruptive and destructive actions legally reserved for the security apparatus of states. Since there are definite differences between the powers of nation states and other organisations, neo-realist contentions can admittedly not be blindly applied to a generic FCCI. These differences between

states and other organisations are accounted for in our FCCI design (Chapter 12, Building Block 7 – Delineation). For the purposes of our discussion in this chapter, we discuss FCCI concepts in generic terms in order to apply them to both the state and *mutatis mutandis* to other organisations. With this qualification, and as long as it is done in an academically sound manner, we deem neo-realism as offering a workable premise to start explaining CCI in general and the FCCI in particular.[4]

Thirdly, we present our 'theoretical anchor' by means of a **layered approach**. We followed this layered approach with the qualification that levels of theory overlap and are mutually supportive. Postulations on the paradigmatic, grand- and meso-theory levels are shown in this Subsection (see Figure 15 on the next page) as well as in Section 5.5 to be abstract and broad in scope. Theories' different purposes are aptly summarised by Gill (2006) in his distinction between "theories of intelligence" and "theories for intelligence". Theories of intelligence, says Gill (2006), are developed to "help academics research intelligence, come to understand it, and better explain it". Theories of intelligence "relate immediately to the needs of practitioners"... In one sense there is no conflict between these two. A good theory of intelligence should, by definition, be useful for intelligence".

Fourthly, we recognise that 'definitions' are essentially a part of theory. In the interest of logical presentation, we offer **denotative definitions** later when presenting Building Blocks 3, 4 and 5 (Chapters 7, 8 and 9). In presenting the theoretical anchor in this chapter, for reasons of simplicity, we delineate concepts enumeratively.[5]

With these qualifications, we can depict the contours of a theoretical anchor as our FCCI's first building block as follows:

Please see next page for Figure 15.

[4] For a detailed discussion on why realism and neo-realism, in our view, best explain intelligence, CI and (by implication) CCI, please refer to Lomans 2017, Duvenage and Hough 2011, and Duvenage 2011. Also see Laksman (2013) for realism and its focus on non-state actors.

[5] Denotative definitions, such as those in dictionaries, describe a concept/object by means of a narrative description. A definition can also be enumerative. In contrast to a denotative definition, an enumerative definition describes the attributes of a concept and in this manner "conveys an 'idea' of the thing defined" (De Vos 2006).

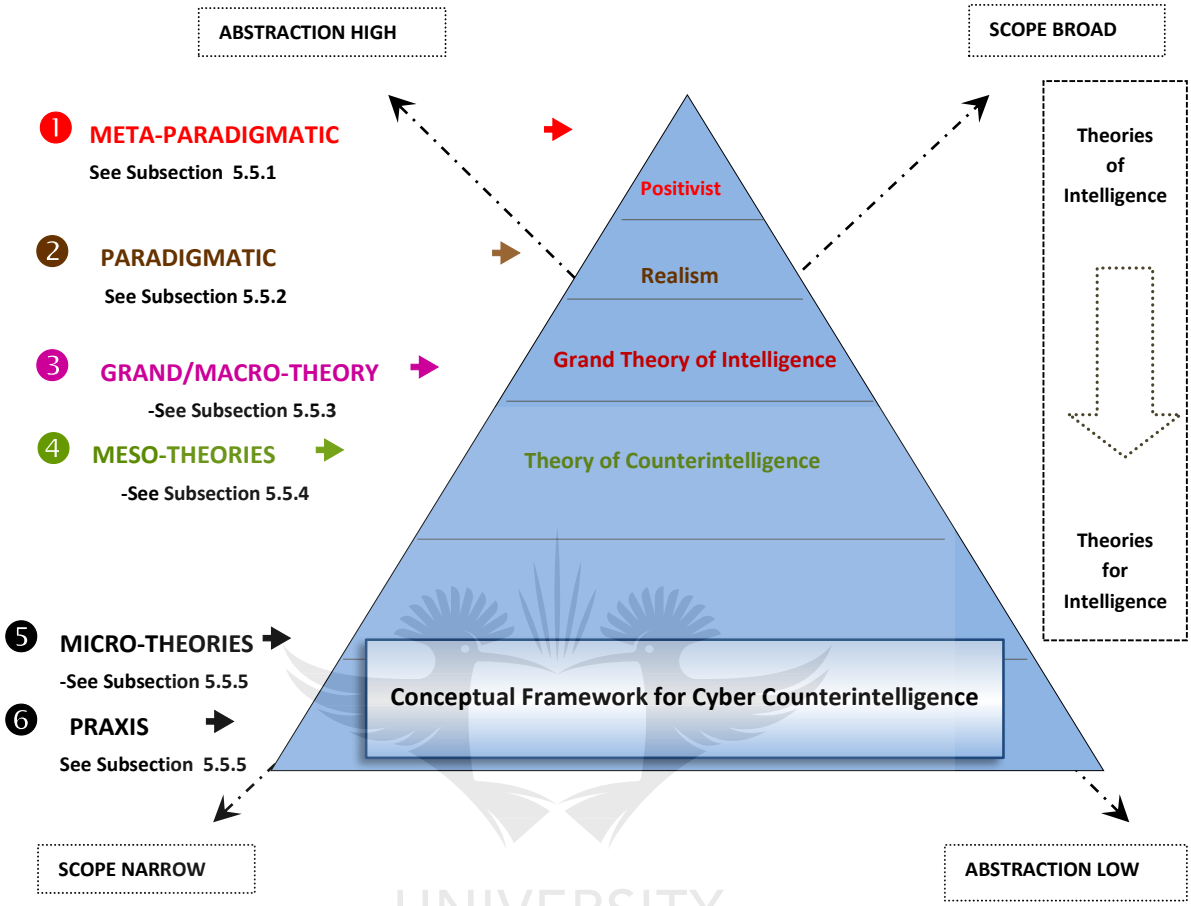


Figure 15: Contours of Building Block 1 – Theoretical Anchoring of the FCCI (adapted from Duvenage 2011 and Duvenage & Hough 2011)

In this section, we outlined our approach to the theoretical anchoring as our FCCI's first building block. We discussed the challenges and qualifications pertaining to such a theoretical contextualisation. We concluded by graphically depicting Building Block 1's contours per Figure 15. In the next section, we discuss this building block in more detail.

5.5 EXPLICATING THE THEORETICAL ANCHOR AS THE FIRST BUILDING BLOCK

In this section, we narratively expound the FCCI's theoretical anchoring as Building Block 1. In line with the graphical depiction (Figure 15), the following aspects are addressed:

(1) Meta-paradigmatic stance – Objectivity and reality (❶ in Figure 15)

(2) Paradigmatic stance: The state's quest for power, survival and prosperity (❷ in Figure 15)

(3) Grand theory: Intelligence as a vital interest and category of state power (❸ in Figure 15)

(4) Counterintelligence as a meso-theory (❹ in Figure 15)

(5) Our framework for Cyber Counterintelligence as a proposition on the micro-theory and praxis levels (❺ and ❻ in Figure 15)

5.5.1 META-PARADIGMATIC STANCE: OBJECTIVITY AND REALITY

As was noted in Section 5.4, we take neo-realism as the theoretical premise for our FCCI. On a meta-paradigmatic level, neo-realism is overlaid on a positivistic stance (see ❶ in Figure 15). Positivism essentially states that an **objective** world (**reality**) exists separately from the researcher/practitioner. Therefore, as researchers and practitioners, we can (relatively) objectively observe and described this reality. Applied to our FCCI, we assert that our framework can relatively objectively identify, describe and guide the proactive mitigation of 'real' threats and risks to the organisation.

5.5.2 PARADIGMATIC STANCE: THE STATE'S QUEST FOR POWER, SURVIVAL AND PROSPERITY

On a paradigmatic level (see ❷ in Figure 15), the neo-realist approach concerns itself with the nation state and its quest for power, survival and prosperity. Central neo-realist contentions are as follows (Taylor 2007; Snow 2004; Sterling-Folker 2006; Hough 2006; Johnson 2003, Duvenage 2011):

- The (nation) state is the primary **referent object** of national security.
- The state is a rational, sovereign and **self-interested** entity driven by the pursuit for national security (**survival and prosperity**).
- The state pursues its interests based on its national **security perception**. This perception is typically embodied in the government's policies, objectives and strategy.
- Interests are pursued in an **anarchic environment** of **intense competition and conflict** with other self-interested actors. Although cooperation between actors

occurs, such cooperation is not of an altruistic nature. It is motivated by the self-centred interests of the respective role-players and will only be sustained for as long as it serves the actors' self-centred agendas.

- Its quest for survival and prosperity requires of the state to protect and expand its **vital interests**. These vital interest are pursued (against other actors) in the political, social, technological, economic, military, ecological (environmental) and informational sectors. Interests in these sectors do not operate in isolation from one another; they overlap and are interdependent.
- The state's **relative power** ultimately determines its success in pursuing its security and interests. This power vests in various categories, of which the most important are political/diplomatic, economic, military and informational. Consequently power is both an aim and a requisite for expanding prosperity and maintaining security.
- While it may offensively strive to maximise its power (**power maximisation**), the state may also opt to defensively pursue **security maximisation** through for example moderate policies.[6]

In this section, our main neo-realist contentions on a paradigmatic level were outlined. In the next section, we extend these contentions to the grand theory level.

5.5.3 GRAND THEORY: INTELLIGENCE AS A VITAL INTEREST AND CATEGORY OF STATE POWER

A grand theory of intelligence should provide a broad understanding of what intelligence is and how it functions (see ❸ in Figure 15). In addition to binding theories on lower levels of abstraction (i.e. meso-, micro- and praxis theories), a grand theory ought to describe intelligence as a phenomenon by presenting overarching similarities and differences in specific contexts of time and place (Treverton *et al.* 2006). As suggested earlier, the road to a theoretical corpus of this nature is proving to be long and the progress incremental. While this discourse is gaining momentum, the following statement by Johnson (2007) still rings true: "Overall, the studies on intelligence theory find that the discipline remains in its infancy, holding great promise for scholars interested in blazing new trails." In a similar vein, Duvenage and Hough (2011) assert:

[6] We duly note that these two positions are, strictly speaking, the opposing contentions of offensive and defensive neo-realist (*cf.* Lomans 2017). For our purposes, however, the positions are not viewed as mutually exclusive.

"So incipient is this discourse that a considerable segment thereof revolves around the methodology and avenues that should be followed in the construction of this road."

While there are some contributions by postmodernist and critical-realist, most attempts to construct a grand theory of intelligence are imbedded in realism (*cf.* Prunckun 2012, Duvenage & Hough 2011, Taylor 2007, Gill & Phythian 2006). It is beyond the scope of this study to review incipient, individual contributions to a **grand theory of intelligence** and we serve the purpose by forwarding some **main contentions** which enjoy relatively broad acceptance in realists (including neo-realist) circles (Prunckun 2012, Johnson 2006, Taylor 2007, Bernhardt 2003, Duvenage 2011):

- Intelligence is underpinned by the **self-centred, power-seeking nature of the state** and the hostility of the environment in which it pursues survival and prosperity.
- Intelligence epitomises **information's dual denotations** in neo-realist theory, namely that it is **simultaneously** a class of **vital interests *and*** a **category of power**.
- On the one hand, information is a class of **vital interest** that the state seeks to protect and advance. This is one of intelligence's primary roles. In fact, intelligence's reason for existence is to provide the state with actionable information on risks, threats and opportunities (Bernhardt 2003). This actionable information includes adversarial secrets.
- One the other hand, information is a **category, and intelligence an instrument, of state power**. In addition to providing actionable information, **intelligence actively engages adversaries** in the information sphere. In providing intelligence and engaging adversaries, intelligence supports and **maximises** the other categories of state power. In this sense, intelligence maximises the state's power in pursuing vital interests in the political, social, technological, economic, military, ecological (environmental) and information sectors. This engagement in the information sphere extends to information warfare. Information warfare and intelligence pursue, in tandem, the goal of "information superiority" (c*f*. Denning 1999, Hutchinson & Warren 2001, Davey & Armstrong 2002 and Duvenage 2011).

In the paragraphs above, we highlighted some neo-realist contentions on a grand theory of intelligence. In the next subsection, we extend this theorisation to CI.

5.5.4 COUNTERINTELLIGENCE AS A MESO-THEORY

Given the incipiency of the discourse on a grand theory of intelligence, contributions on CI theory is unsurprisingly even more limited (see 4 in Figure 15). Notable attempts are those of Prunckun (2012, 2014), Duvenage (2011), Taylor (2007), and Shulsky and Schmitt (2002). All the cited attempts ascribe to realism/neo-realism and are built on the notion that CI is an element of intelligence. This is aptly summarised by Shulsky and Schmitt (2002): "Once we understand that intelligence is part of a struggle between countries, we see why counterintelligence is not an afterthought but is rather an integral part of it."

Applied *mutatis mutandis* to the context of this study and an organisation, four **neo-realist assumptions** (applied to an organisation) underlying the existence of CI as proposed by Taylor (2007) and described in Duvenage (2011) are:

(1) An organisation possesses information that if compromised to an adversary will negatively impact its security.
(2) An organisation has an intelligence capacity/structure(s) that collects and analyses information. The organisation strives to protect this information from unauthorised disclosure and tampering.
(3) Adversaries attempt to access other organisations' information/intelligence.
(4) A low level of trustworthiness must be assumed in respect of most people.

Moving from and adding to these assumptions, recent neo-realist contributions posit CI as having the primary missions of offense and defence (*cf.* Prunckun 2012, Duvenage 2011, Taylor 2007, Shulsky & Schmitt 2002). The defensive and offensive missions [7] are viewed as distinguishable but inseparable. They function in synergy to execute two primary foci (Duvenage 2011; Prunckun 2012, 2014):

- **Focus 1**: CI's first focus is to protect, defensively and offensively, the integrity of the own vital informational interest.
- **Focus 2**: CI aims to compromise the informational integrity of adversaries. Like intelligence, CI is thus part of informational power. As reflected in our later discussions on CI as a building block of our FCCI (Chapter 8), the interlink between CI's foci and its missions remains poorly understood up to this day.

[7] Offensive and defensive missions are not identical to, and should not be confused with, the earlier discussed offensive and defensive neo-realist theorisation streams.

In this section, we outlined some contours of a neo-realist theory of CI. Since our later discussion (in Chapter 8: Building Block 4 – Counterintelligence) expands and concretises the foregoing theory as an FCCI building block, this subsection was very condensed in its overview. In the next section, we explain our FCCI as a postulation on the micro- and praxis theory levels.

5.5.5 OUR FRAMEWORK FOR CYBER COUNTERINTELLIGENCE AS A PROPOSITION ON THE MICRO- AND PRAXIS THEORY LEVELS

To reiterate, our FCCI is a theory of intelligence since it pertains to the immediate needs of practitioners. In a finer distinction, theories of intelligence can be divided in micro- and praxis theories (*cf.* Duvenage & Hough 2011, Duvenage 2011). Micro-theories typically deal with a specialised area of expertise in a manner which link practice with theories on higher levels of abstraction (i.e. with grand and meso-theories). As suggested by the term, 'praxis' postulations describe concretely the TTTPs employed in practice. (See ❺ and ❻ in Figure 15.)

In addition to dovetailing praxis with higher theories, **micro-theory**'s purpose is to provide a **'scaffold'** to structure existing knowledge and aid further research on the execution of a specialisation field – in this case CCI. As we explained in Chapter 2 (Section 2.2), our FCCI is a conceptual framework with precisely this purpose. However, our FCCI is not a 'pure' micro-theory. It is also a model to be used in performing 'actual' CCI work practically (praxis). In explaining our FCCI later on, CCI TTTPs (process) are detailed in Chapters 9, 10, 11 and 13. In this respect, our **FCCI** therefore also contains elements of **praxis** postulations. (This is depicted in ❺ and ❻ in Figure 15.)

In this section, we explained our FCCI as a theoretical proposition that spans the micro- and praxis levels. This proposition is the final contour of our FCCI's first building block.

5.6 SUMMARY AND CONCLUSION

In this chapter, we set out to present a **theoretical anchor** as our **FCCI's first building block**. We emphasised that to be academically credible and practically useful, the FCCI has to be duly considered and positioned as part of the existing theoretical discourse. Such anchoring *inter alia* provides a nexus for linking CCI with other academic fields.

To this end, we contoured Building Block 1 by discussing various levels of theory ranging from the meta-paradigmatic to the praxis level. Albeit very cursory, we illustrated the way in which our thinking on higher levels of abstraction (meta-, paradigmatic, grand and meso-levels) impacts our approach to the functional and practical levels (i.e. micro- and praxis level).

With our FCCI theoretically anchored, we now proceed to the next chapter, where we discuss the organisation as Building Block 2.

CHAPTER 6

BUILDING BLOCK 2 – ORGANISATION

6.1 INTRODUCTION

If 'theory' is our FCCI's anchor, then the **organisation** is its **pivot**. Ultimately, and as will be shown in the rest of this and other chapters (notably Chapters 9–13), **CCI exists because of and for the organisation** it serves. As was observed in Chapter 5 (Section 5.4) 'organisation' - within the context of its use here - is an **extendable term** which could denote state actors, non-state actors (e.g. business, criminal, terrorist and activist entities) and even individuals. Therefore, the nature of the organisation and its needs shape the CCI endeavour. Clearly then, we cannot conceptually structure and understand CCI if we do not understand the organisation it serves. Accordingly, in this chapter, the organisation is advanced as our FCCI's second building block. Graphically, the addition of the organisation as our FCCI's pivot and Building Block 2 can be depicted as follows:

Figure 16: Building Block 2 – Organisation (Duvenage, Sithole & von Solms, 2017)

To present the organisation as our FCCI's second build block, the rest of this chapter is structured as follows:

- Section 6.2: Organisation – Why it is needed and important as a building block
- Section 6.3: Central aspects pertinent to the organisation as a building block
- Section 6.4: Demarcating the organisation's informational interests
- Section 6.5: Organisational risk management and its relation to CCI
- Section 6.6: Summary and conclusion

6.2 ORGANISATION – WHY IS IT NEEDED AND IMPORTANT AS A BUILDING BLOCK

The organisation is advanced as the FCCI's pivot and second building block for reasons of theory and practicality.

In line with our neo-realist theoretical position, the organisation and the pursuance of its interests predominate. Seen through this lens, CCI is ultimately about maximising the organisation's power by protecting and advancing its interests. Therefore, and as mentioned earlier (Section 6.1), CCI exists because of and for the organisation it serves. In applying the neo-realist notion, we view the organisation as a self-interested actor driven by the need to secure and expand its interests. The organisation does this in conflict and competition with other actors (adversaries) and in a hostile environment.

Also practically, effective CCI crucially depends on profound knowledge of the organisation. If treated as an 'add-on' or 'plug in', CCI will imperil rather than benefit the organisation it is supposed to benefit. Effective CCI needs to be part of the **organisational 'DNA'**. Consequently, **sound CCI does not start with on-the-network actions; it starts with a profound understanding of the organisation itself, its strategy, its competition and the environment in which it operates**. Against sophisticated adversaries, for example, the organisation's staging of honeynets and the content filling of honeypots, honeyfiles and honeytokens have to be attuned to the organisation itself, its adversaries and its environment (Bodmer *et al.* 2012; Duvenage, Sithole & von Solms 2017). Clearly then, CCI is not an afterthought to, but an integral part of, organisational strategy Intelligence and CI. Graphically, this synergetic dynamic can be depicted as follows:

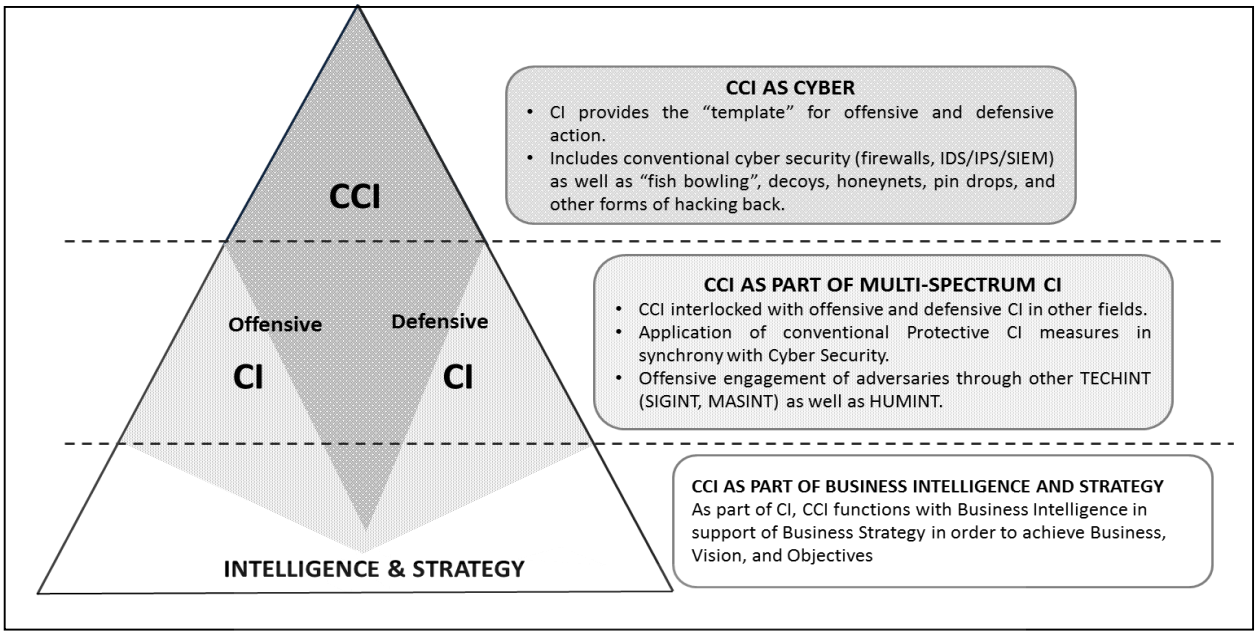


Figure 17: CCI in the context of Strategy, Intelligence and Counterintelligence (Duvenage & von Solms 2014)

As neo-realism puts the state at the centre of security and prosperity, our FCCI posits the more generic concept of an organisation as the pivot of the framework. This understanding shapes CCI on all levels, namely strategic, operational, tactical and technical. (See Chapter 11 for a discussion of these different CCI levels within the organisation.) The positioning of the organisation as the FCCI's second building block furthermore provides a nexus for contributions to CCI from other academic fields such as Business Studies and Management Science.

6.3 CENTRAL ASPECTS PERTINENT TO THE ORGANISATION AS A BUILDING BLOCK

Since the aforementioned CCI levels are discussed in more detail in Chapter 11, we can for our purpose here assert in more general terms that the design of the CCI endeavour starts with clear understanding of the following **organisational aspects** (see Duvenage 2011):

- The organisation's **vision, objectives and strategy** which in effect concretise the vital interests that the organisation aspire to protect and procure in order to be more safe and prosperous.
- Organisational **strengths** (including the vital interests it possesses) and **weaknesses** (vulnerabilities).

- The **environment** in which the organisation functions. Of particular importance are the actual/potential **impact** of current, as well as anticipated trends, in the organisation reaching its objectives and expanding its prosperity. Since it will decisively influence the organisation's CCI endeavour; the legal, regulatory and governance context within which the organisation operates is equally important. (See Section 6.4 and Building Block 7: Delineation *per* Chapter 12, Subsection 11.3.1)
- Actual and potential **competitors/adversaries** and, in this instance, the implications/impact thereof for the organisation attaining its objectives.

Moving from these central organisational aspects, the next section reflects on the importance of demarcating an organisation's informational interest.

6.4 DEMARCATING THE ORGANISATION'S INFORMATIONAL INTERESTS

An understanding of the above mentioned general aspects is foundational to ascertaining what ought to lie at **the heart of intelligence, CI and CCI efforts**, namely clear demarcating what the organisation's informational interests are. These **informational interests**, to apply the neo-realist theory forwarded earlier in this chapter as well as in Chapter 5, comprise the following interrelated facets (as described in Duvenage 2011):

(1) Informational interests encompass the **informational assets** which the organisation **possesses**, values and protects. This encompasses the whole body of information at the organisation's avail that is necessary for its survival, prosperity as well as the expansion of its vital interests in other areas. These informational assets are of both a tangible and intangible nature, and denote the systems, institutions, processes and people that gather, store, process, communicate and otherwise use information.

(2) Informational interests refer to the (informational) **assets the organisation aspires to procure** (such as information on, and secrets of, adversaries or better technology to protect itself).

(3) Informational interests pertain to the **conditions** that the organisation seeks to **maintain or realise** (e.g. gaining a competitive edge over an adversary by obtaining information, augmenting the organisation's own informational security or undermining the informational integrity of an adversary through deception).

The informational interests outlined in this section are not mere theoretical notions of academic significance only. The FCCI's subsequent building blocks concretise these interests to the essential end goals directing organisational strategy, intelligence, CI and CCI.

6.5 ORGANISATIONAL RISK MANAGEMENT AND ITS RELATION TO CCI

Chapters 7 to 13 will show intelligence, CI and CCI to for a substantial part entail the identification, anticipation and mitigation of risks to organisations. Various terms used in in these chapters are commonly associated with the multi-disciplinary field of risk management and include: 'threats' 'vulnerabilities' 'assets' and 'impact' (Bernhardt 2003; Ruighaver Warren & Ahmad 2011, Duvenage 2011, Harvard 2018). While risk management is not new to Intelligence studies and Information Security (Bernhardt 2003, Ruighaver Warren & Ahmad 2011, Duvenage 2011), it has been gaining traction in recent years within the cybersecurity field specifically. Attesting to this trend is the offering of courses such as Harvard University's short course certificate in cybersecurity risk management (Harvard 2018). The said course culminates in the compilation of an organisational cyber risk mitigation strategy which has the following elements (Harvard 2018):

- Organisation's vision (for implementing a cyber-risk mitigation strategy)
- Organisation's 'strategic goals and objectives (to reduce risks)
- Metrics
- Threat actors and methods of attack
- Business critical assets (systems, networks and data)
- Cybersecurity governance and leadership
- Protective technologies
- Legal considerations
- Incident response plan.

All of the above-noted risk mitigation elements are indispensable in moving from a reactive to proactive cybersecurity posture. As suggested earlier, risk identification mitigation and management are central to intelligence, CI and CCI. Accordingly, 'threats', 'vulnerabilities', 'impact 'and 'risks' feature prominently in the CCI process we advanced in Chapter 13. (**The reader is requested to now compare Figure 41 on page 142 of the thesis**.) However, as Figure 41 and other subsequent chapters will

show, CCI goes beyond proactive risk management in that it also aims to (1) identify and exploit opportunities; and (2) adds an offensive dimension to both active and passive modes. CCI does so, to reiterate one of the thesis's recurring themes, as part of the organisational strategy as well as its intelligence and CI endeavours. CCI thus stands in a symbiotic relationship with organisational risk management as these as are distinguishable yet inseparable constructs.

In this section we discussed the relationship between organisational management and CCI. We now proceed with reflecting on the impact of organisational type on CCI.

6.6 IMPACT OF ORGANISATIONAL TYPE ON THE CYBER COUNTERINTELLIGENCE ENDEAVOUR

The nature of an organisation will self-evidently shape its **vision, objectives strategy,** informational interests and security posture. The security posture of a non-state actor (e.g. publishing company) would, for example, in various respects differ from that of a state actor (e.g. statutory intelligence service). Organisational type thus shapes the whole of the CCI endeavour from 'soft' issues such as organisational CCI awareness (Chapter 14) to the sharp offensive cutting end of CCI operations (Chapters 9, 10, 11 and 13). For this reason, the delineation of the CCI endeavour in accordance with the organisational type is of the utmost importance.

6.7 SUMMARY AND CONCLUSION

This chapter advanced the organisation as the FCCI's second building block. We commenced with stating the academic and practical imperatives for postulating the organisation as the FCCI's pivotal building block. We proceeded with discussing aspects central to configuring this building block such as organisational vision, objectives and strategy. Subsequently, the importance of demarcating organisational informational interests and relationship between CI and organisational risk management were discussed. We then reflected very cursory on the impact of organisational type on the CCI endeavour.

Of course, CCI does not ascertain and pursue an organisation's informational interests by and for itself. This is done as part of an organisation's intelligence endeavour. In the next chapter, we therefore propose intelligence as the FCCI's subsequent building block.

CHAPTER 7

BUILDING BLOCK 3 – INTELLIGENCE

7.1 INTRODUCTION

In Chapter 6, we posited the organisation as Building Block 2 and the pivot of our FCCI. Now we move forwards to Building Block 3, namely an organisation's intelligence endeavour. We cannot conceptually structure and understand CCI if we do not understand intelligence, of which CCI forms part. To this end, this chapter is structured as follows:

- Section 7.2: Intelligence – Why it is needed and important as a building block
- Section 7.3: Essential contours of intelligence as a building block
  - Subsection 7.3.1: Contour 1 – Definition of intelligence
  - Subsection 7.3.2: Contour 2 – Intelligence trident (elements)
  - Subsection 7.3.3: Contour 3 – Intelligence functions
  - Subsection 7.3.4: Contour 4: Intelligence conduits
- Section 7.4: Conclusion

Graphically, the addition of intelligence as an FCCI building block can be depicted as follows:

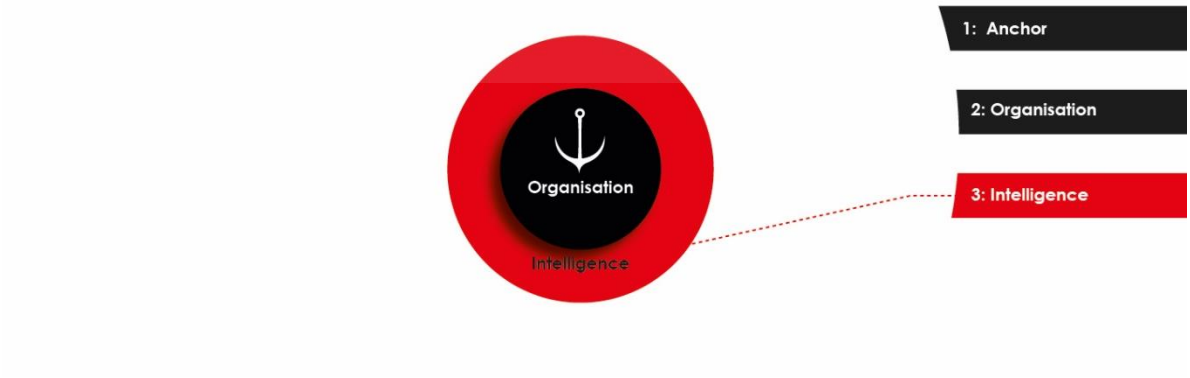


Figure 18: Building Block 3 – Intelligence (Duvenage, Sithole & von Solms 2017)

7.2 INTELLIGENCE – WHY IT IS NEEDED AND IMPORTANT AS A BUILDING BLOCK

While it is an indispensable organisational instrument, we concluded in Chapter 6 (Section 6.4) that **CCI cannot secure and pursue an organisation's interests all by and for itself. This has to be done as part of an organisation's intelligence endeavour**. CCI, by way of analogy, is but one 'tool' within an organisation's intelligence 'toolkit'. Academia and practitioners who are serious about CCI therefore have to have a sound grasp of the intelligence 'toolkit' as well as intelligence's three respective 'toolsets', namely the elements of positive intelligence, covert action and CI. While essentially part of CI (discussed in Chapter 8), CCI benefits and is dependent on positive intelligence and covert action. In a similar vein, effective CCI depends on all the major intelligence functions such as management, analysis and collection. Therefore, these intelligence elements and functions have to be part of the construction of our FCCI.

A thorough exploration of the notion 'intelligence' is important to this study because CI and CCI are extensions of the own organisation's intelligence endeavour. To a significant degree, CI and CCI are about engaging and countering **hostile intelligence** activities. By examining the notion 'intelligence', we **will thus also be better at understanding that which CCI engages and counters – namely hostile *intelligence* actions**. A thorough examination of the concept 'intelligence' will therefore aid the explanation of CI and CCI later on in this thesis.

In this section, we explained the importance of intelligence as Building Block 3 of our FCCI. In the next section, we expound this building block.

7.3 ESSENTIAL CONTOURS OF INTELLIGENCE AS BUILDING BLOCK 2 OF THE FCCI

As reflected in Section 7.2 (Paragraph 1), intelligence is a multifaceted endeavour but only its most salient and relevant features can be touched on in this thesis. In the interest of simplicity, we have identified four aspects of intelligence critical to understanding and informing effective CCI. For our purposes, we present these aspects as the essential contours of intelligence – and thus **the contours of the third building block of our FCCI**, namely:

- Contour 1: Definition of intelligence

- Contour 2: Intelligence trident (i.e. the three intelligence ‘toolsets’)
- Contour 3: Intelligence functions
- Contour 4: Intelligence conduits

We now proceed with discussing each of these contours and in doing so, expound this building block.

7.3.1 CONTOUR 1: DEFINITION OF INTELLIGENCE

Within Intelligence Studies, the term 'intelligence' is hotly contested and there is no single definition which is universally accepted. Over decades, and within statutory intelligence circles, there has however developed relatively broad-based agreement with Kent's (1949, 1966) seminal assertion that 'intelligence' denotes a specific type of "knowledge", "organisation" and "activity", and the combination of these three (Kent 1949, 1966).[8] Few would dispute the notion that 'intelligence' relates to actionable knowledge provided to an organisation by a structure established for this purpose (Godson 2001). In emphasising the activity facet of intelligence, Lowenthal (2012) offers the following useful "working concept" for describing intelligence:

> Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers, the products of that process; the safeguarding of this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.

As noted earlier (Chapters 1 and 5) our aim is that the FCCI should be an instrument with wider application than just nation states and their governments and intelligence structures. Therefore, we have to formulate a definition relevant to the generic concept

[8] In his book *Strategic intelligence for American world policy*, Kent (1949) pioneered the idea of intelligence as “knowledge”, “organization” and “activity”. Contemporised by various authors (Lowenthal 2010; Johnson 2004; Shulsky & Schmitt 2002), the three facets identified by Kent essentially remain the core of current descriptions. Kent positioned intelligence as that “specialized knowledge” which is indispensable to a nation state’s “welfare and security” (Kent 1949, 1966). This specialised knowledge is produced by a state structure(s) of “living people” that is institutionally geared towards delivering such knowledge (Kent 1949, 1966). The organisation acquires and provides the specialised knowledge through the execution of certain activities such as collection and analysis (Kent 1949). In a more comprehensive sense, intelligence can lastly be seen as a combination of the three facets mentioned above.

of an organisation which will tie intelligence to the preceding Building Blocks 1 and 2. With this in mind, we **define our FCCI's 'intelligence' building block** as follows:

> Intelligence is the process by which specific types of information important to an Organisation's vital interests (security and prosperity) are requested, collected, analysed, and provided to the decision makers, the products of that process; the safeguarding and advancement of informational interests by counterintelligence activities; and the carrying out of other sanctioned informational operations.

In this Subsection, we advanced a definition of intelligence as Contour 1 of our FCCI's intelligence building block. In the next subsection, we further explain intelligence by means of Contour 2, the intelligence trident (elements).

7.3.2 INTELLIGENCE CONTOUR 2: INTELLIGENCE TRIDENT (ELEMENTS)

Implicit to Lowenthal's (2010) definition above (Subsection7.3.1) is the notion that until recently enjoyed near axiomatic acceptance in Intelligence Studies. This axiom holds that intelligence comprises four "major elements" (also referred to as "functions" and "disciplines"), namely collection, analysis, covert action and CI (Codevilla 1992; Godson 2001). For various reasons, this subcategorisation of intelligence into these four elements is more confusing than helpful (Van den Bergh 2015; Duvenage & Hough 2011). For one, this subcategorisation does not assist in clarifying the juxtaposed use of 'intelligence' as an abbreviated reference to the concept 'positive intelligence' (Duvenage, von Solms & Corregedor 2015; Sims 2009; Bodmer *et al.* 2012; Duvenage & Hough 2011). This categorisation is furthermore not attuned to contemporary intelligence practice (Duvenage, von Solms & Corregedor 2015; Duvenage & Hough 2011) and consequently **not useful to describe the intelligence building block of our FCCI**.

To simplify and clarify intelligence's elements, we ascribe to an alternative proposition advanced by Duvenage and Hough (2011) and later developed for application to CCI by Duvenage, von Solms and Corregedor (2015). This proposition distinguishes between intelligence elements (positive intelligence, covert action and CI) and intelligence functions (such as management, analysis and collection). Accordingly, we now discuss the intelligence elements as the second contour and intelligence functions as the third contour of Building Block 3.

We posit intelligence as consisting of three main elements, namely positive intelligence, covert action and CI. Collectively, the elements constituting the intelligence trident can graphically be depicted as follows:

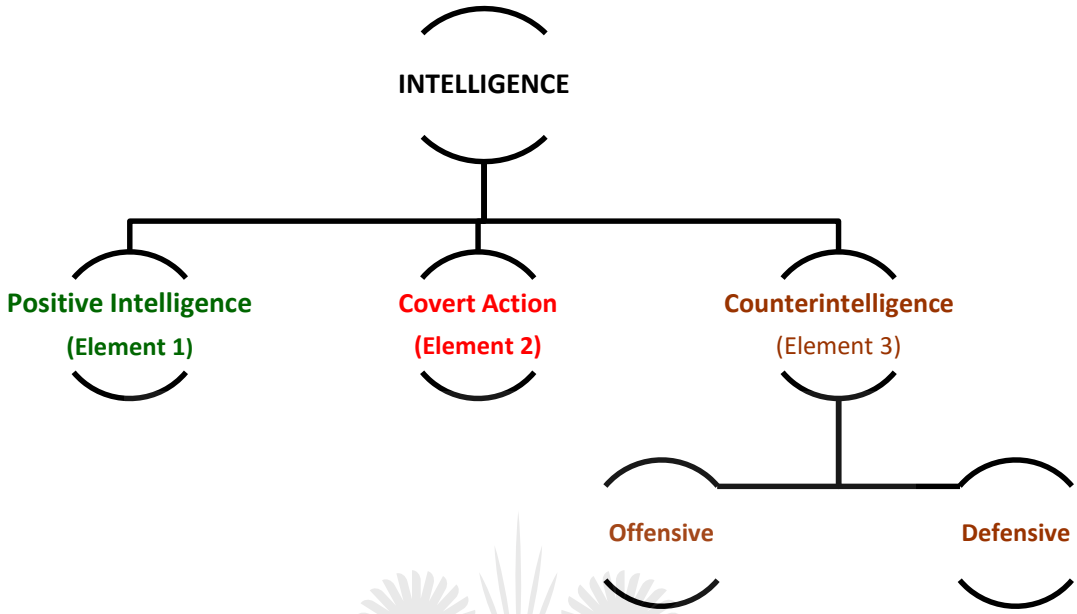


Figure 19: Intelligence Trident (Duvenage, von Solms & Corregedor 2015)

In narratively explaining this graph, the main elements can concisely be described as follows (Duvenage, von Solms & Corregedor 2015):

- **Element 1. Positive intelligence** is primarily aimed at providing information "to facilitate one's own side achieving its ends" (Bodmer *et al.* 2012). This information varies from analysed open sources to an opponent's secrets obtained through espionage. As noted above, 'intelligence' is frequently used interchangeably as referring to 'positive intelligence', with the context determining what meaning is implied (Sims 2009). From our explanation in the two bullet points directly following this one, it is abundantly clear that intelligence is about much more than delivering actionable knowledge about opponents and the environment. It also entails covert action and CI – whether executed by state or non-state actors..
- **Element 2. Covert action** targets an adversary by influencing events, conditions, individuals, groups or institutions to the benefit of the client and in a manner not attributable to the sponsor or at least offering plausible deniability (Duvenage, von Solms & Corregedor 2015). To this end, measures instituted "are to one degree or another secret (hidden) or covert (disguised)" (Godson 2001). In the context of **state security**, covert action can include action such as military and intelligence interventions and support. In **state intelligence** structures, covert action mostly

relates to informational actions such as propaganda, deception and disinformation (Godson 2001). In the business environment, some forms of deception and “perception management” could in effect be forms of covert action (Francq 2000).

- **Element 3. CI** is an abbreviated form of countering hostile intelligence activities. CI defensively and offensively guards against adversarial intelligence (i.e. hostile positive, CI and covert action) operations (Duvenage, Von Solms & Corregedor 2015; Prunckun 2012; Sims 2009). CI thus pertains to the safeguarding of the own organisation's weaknesses and vulnerabilities as well as the active engagement of adversaries.

It must be emphasised that the above elements should not be construed as silos. Intelligence involves the execution of these primary elements in a mutually supportive and overlapping manner. For example, CI (and thus CCI) not only safeguards the positive intelligence and covert action elements, but delivers information useful to both. Similarly, positive intelligence renders information of high relevance to CI/CCI. CI/CCI in turn relies on (informational) covert action to degrade adversarial intelligence efforts.

In explicating **intelligence as a building block of our FCCI**, we have in this subsection discussed the three primary intelligence elements as the second contour. We explained the relation between CI and other elements. This relation is relevant to the **construction of our FCCI since effective CCI, as a subset of CI, depends on synergy with the positive intelligence and covert action elements**. In the next subsection, we explain some intelligence functions which bind, and are performed, in all the three intelligence elements (see Figures 19 and 20).

7.3.3 INTELLIGENCE CONTOUR 3: INTELLIGENCE FUNCTIONS

The intelligence functions which bind, and are performed, in all the three intelligence elements constitute the third contour of our FCCI’s intelligence building block. Such specialised **intelligence functions**, which are also performed in CCI, were noted in Subsection 7.3.2 to include management, analysis and collection. These functions are critical to ensure that intelligence (and thus CCI) is aligned with, and executed to the optimal benefit of, the organisation. Phrased differently, these **functions** synergise the intelligence elements (**positive intelligence**, **covert action** and **CI)** to optimally pursue an organisation's interests, goals and strategy (**IGS**). Diagrammatically this relationship can be depicted as follows:

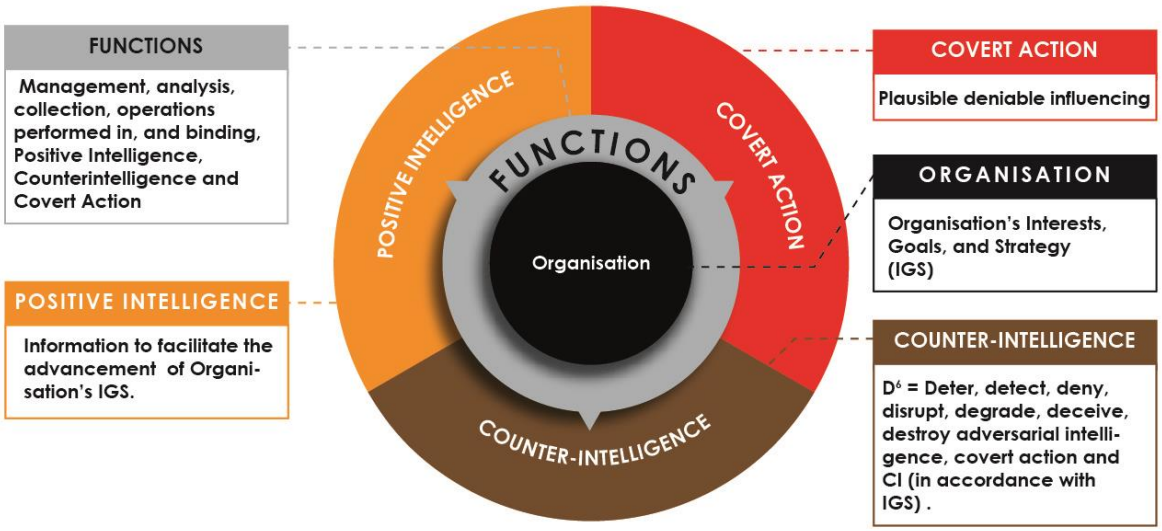


Figure 20: Positioning of Intelligence Functions (Adapted from Duvenage, Sithole & von Solms 2017)

Of these functions, analysis and collection are performed by the **own organisation** as part of the **collective intelligence process** and within all the respective elements. Conversely, when collection and analysis are performed by adversaries, these functions are **countered by the own organisation's CI and CCI effort**. Since an understanding of these functions is pertinent to subsequent building blocks of the FCCI, we now discuss the collection and analysis functions in more detail.

(1) Collection

Collection refers to the procurement of information from three primary categories of sources, namely open, grey and clandestine sources. **Open-source** intelligence (OSINT) pertains to information that is publicly and freely available, such as in newspapers and books, on the surface web, in academic journals and publications, as open-source high resolution imagery, in radio and television broadcasts, on certain governmental databases, in business reports and the like (Quiggin 2007). In the cyber realm, some forms of threat intelligence are open sourced.

Opinions on what **grey collection** comprises are divided (Steele 2007). For our purposes, collection of information from grey sources pertains to those not freely available, though not (a) requiring the employment of clandestine methods and (b) the targeting classified sources. The use of databases, privileged in the sense that payment

for access is required, serves as an example. Within the cybersphere, customised threat intelligence platforms and streams are deemed as grey sources. Grey-sources also include information generated by methods not illegal and clandestine but in some instances *male fide*.

Clandestine or **secret collection** pertains to the procurement of secret or proprietary information without the sanction of the owner(s) and typically in a manner seeking to avoid detection (i.e. obfuscating the collection effort and/or its real intentions). Although it is somewhat of an oversimplification, by far the larger part of clandestine/secret collection of information can be described by the term '**espionage**'.

The result of the whole collection effort, which combines all three collection categories, is referred to as all-source information. **Effective CCI**, as will be shown in Chapter 13, **has integrated all-source information at its core**.

(2) Analysis

All-source information, however comprehensively and widely gathered, is just that – information and not intelligence. Information in its raw form has limited utility value and is subjected to a second intelligence function, namely analysis. Analysis involves the conversion of collected information into descriptions, explanations, assessments and conclusions (Bernhardt 2003). The analysis product is delivered to clients in written format or verbally (Bruneau & Dombroski 2004). As elaborated on in Chapters 10, 11 and 13, the products emanating from **CCI analysis** can be stratified as being on the tactical, operational and strategic levels.

These levels mirror the organisational layers on which statutory security structures (as well as other state and non-state entities, such as businesses) often function. Tactical intelligence is mostly descriptive, directed to line functionaries and is focused on immediate situations and actions. Operational intelligence deals with the assessment of CCI programmes, operations and projects. It is, for the most part, directed to middle management. Strategic intelligence is broader in scope, usually integrating several sources of information and has as its aim to inform the executive management. The outcome of the analysis process therefore directs the organisation internally and externally. This is especially true in CI and CCI (see Table 7 in Chapter 11).

The information collected and analysed to produce intelligence is typically derived through a combination of two primary conduits, namely human and technical. Several

recent 'cyber' breaches have illustrated role-players to have employed cyber measures in tandem with other technical and human intelligence conduits The ongoing revelations by the whistleblower Edward Snowden on the Five Eyes intelligence activities as well as the 2016 breach of the US Democratic Party Convention are but two examples (Duvenage & von Solms 2015; Duvenage, Sithole & von Solms 2017). The unpacking of these conduits is therefore clearly essential to the contouring of intelligence as the intelligence building block of our FCCI and is discussed in the next subsection as Contour 4: Intelligence conduits.

7.3.4 INTELLIGENCE CONTOUR 4: INTELLIGENCE CONDUITS

As noted above, information collected and analysed to produce intelligence products is typically derived through a combination of the human and technical conduits/vectors. If used with the 'positive intelligence' denotation, these vectors are referred to by the acronyms HUMINT (human intelligence) and TECHINT (technical intelligence). What is sometimes overlooked (as suggested in Subsection 7.3.3) is that **these conduits are also the vectors for executing** the other intelligence elements, namely **covert action** and **CI** (*cf.* Lowenthal 2012, Bruneau & Dombroski 2004). An intelligence structure could, for example, use a human asset to gather positive intelligence (spying), conduct covert action (agent of influence) and perform a CI role (double agent). In a similar vein, various fields in TECHINT can serve the purposes of positive intelligence, CI and covert action.

The cybersphere (as shown in Table 3 below) is but one such TECHINT field. Other overlapping TECHINT fields include signal intelligence (SIGINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT). Although the taxonomy of TECHINT is useful to conceptualise TECHINT and contextualise cyber intelligence (CYBINT), these TECHINT fields are for the most part closely interlinked and overlapping. With this qualification, the following table contains a taxonomy of prominent TECHINT fields.

Table 3: Taxonomy of TECHINT Fields (adapted from Duvenage 2011)

SIGINT		
SIGINT essentially refers to the interception of various types of electronic signals. Some forms of SIGINT (explained below) are COMINT, ELINT, FISINT and TELINT.		
Communication intelligence	COMINT	Interception of communications between two or more parties.
Electronic intelligence	ELINT	Interception of (non-communication) electronic signals, such as radar and navigation systems.
Foreign instrumentation signals intelligence	FISINT	Monitoring of electronic magnetic emissions, notably pertaining to aerospace, surface and subsurface systems.
Telemetry intelligence	TELINT	Collection of data streams relayed by systems on, for example, their location, speed, status and other performance metrics. TELINT therefore constitutes a subcategory of FISINT.
IMINT		
In its most basic form, IMINT can be viewed as information gleaned from 'pictures'. Such pictures can be conventional photographs (PHOTINT) or imagines based on spectrum radiation (e.g. infrared). IMINT can be collected by, among others, satellites (SATINT), conventional aeroplatforms (such as airplanes) and unmanned aerial vehicles.		
MASINT		
Lowenthal (2012) aptly remarks on the "arcane debate that rages" between those who view MASINT as a distinctive technical collection subdiscipline, and others who consider it "simply as a product, or even by-product, of SIGINT and other collection disciplines". Basically, MASINT refers to information gathered and analysed as it pertains to a 'signature' (such as emissions, sounds, radiation and movement). Indicated below are some of the vast array of 'MASINTs':		
LASINT	Laser intelligence	
DMPINT	Dynamic measurement photography	
IRINT	Infrared intelligence	
ELECTRO-OPINT	Electronic, optical intelligence	
CYBINT		
CYBINT is information derived from and pertaining to computers, computer networks and systems. Since computers (of varying complexity and capacity) are increasingly imbedded in other systems, CYBINT overlaps with all technical fields.		

Read with Section 7.3, Table 3 will enable us to contextualise and (in Chapter 9) employ CCI as part of the boarder intelligence endeavour. Table 3 is also central to a meaningful understanding of our definition of CCI in Section 9.3 (Chapter 9), where we state that CCI pertains to the engagement of adversarial intelligence actions where cyber is a primary conduit (i.e. CYBINT) and/or where cyber assets are targeted through TECHINT or HUMINT. With a view to our discussion in Chapter 9, we can graphically summarise this Section and contextualise both CYBINT and CCI as follows:

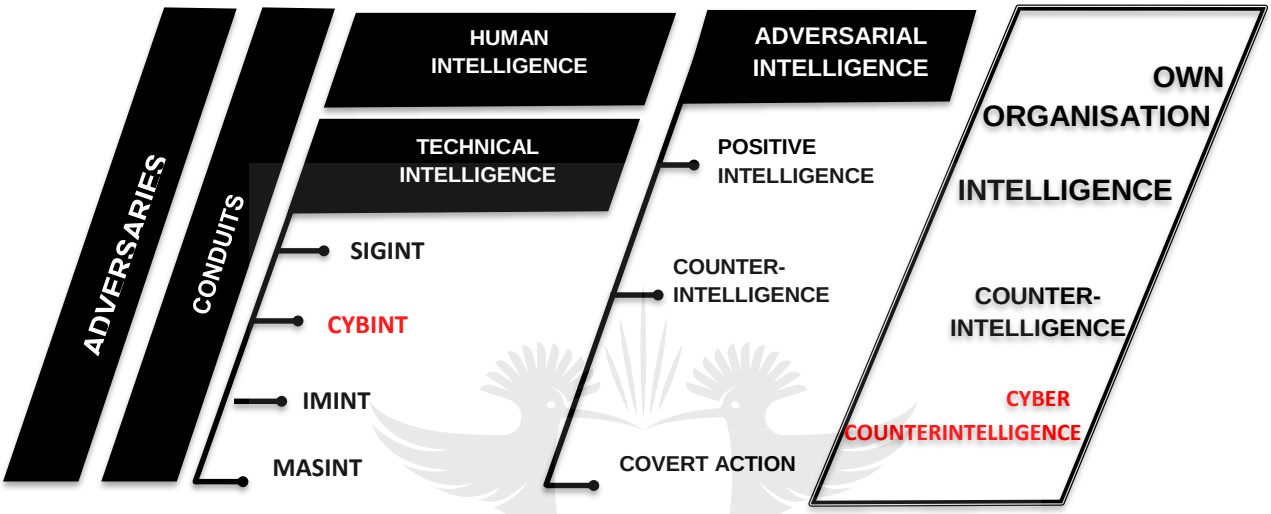


Figure 21: CYBINT and CCI in the Context of Intelligence (Author)

7.4 CONCLUSION

In this chapter, we advanced intelligence as a building block of our FCCI.[9] We conceptually structured intelligence by providing the four contours: (1) a definition, (2) the intelligence trident (elements), (3) intelligence functions and (4) intelligence conduits. We emphasised that CCI is executed within the context of the own organisation's intelligence endeavour. Likewise, CCI is central to countering the whole of the adversarial intelligence endeavour. In both respects, the importance of performing CCI in synergy with multidisciplinary CI cannot be overstated. Therefore, CI is advanced in the next chapter as a distinctive building block of our FCCI.

[9] This chapter is based on, and contains verbatim extracts from Duvenage 2011, Duvenage & Hough 2011, Duvenage 2013, and Duvenage, von Solms & Corregedor 2015.

CHAPTER 8

BUILDING BLOCK 4 – COUNTERINTELLIGENCE

8.1 INTRODUCTION

In the preceding chapter, we pointed out the critical importance of CCI being understood and performed as part of multidisciplinary CI. In this section, we advance CI as the subsequent building block of our FCCI. We can, after all, not conceptually structure and understand CCI if we do not understand CI, of which CCI is part. As is depicted in the figure below, this building block includes a four-sector CI matrix with offensive–defensive and passive–active axes.

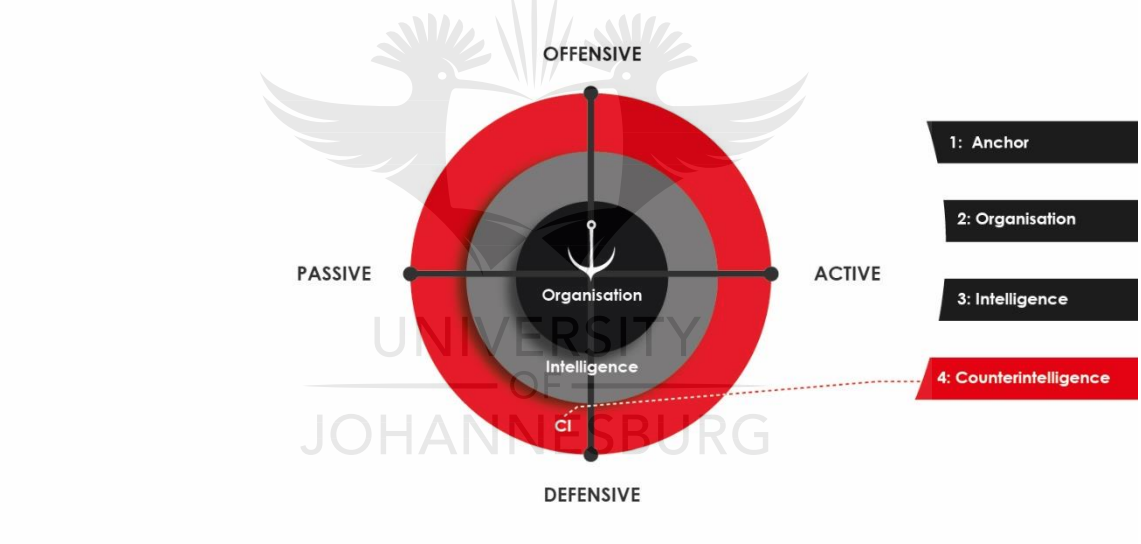


Figure 22: Building Block 4 – Counterintelligence (Duvenage, Sithole & von Solms 2017)

In respect of this chapter's structure, discusses the need and importance of CI as a building block of the FCCI in **Section 8.2**. **Sections 8.3 to 8.5** are then devoted to explicating CI as Building Block 4 of our FCCI. This is done by discussing the **three contours** we deem essential to explaining CI, namely:

- Contour 1: Definition of counterintelligence (Section 8.3)
  - Counterintelligence as a contested concept (Subsection 8.3.1)
  - Working definition of counterintelligence (Subsection 8.3.2)

- Contour 2: Notional structure and principles of counterintelligence, which include a four-sector counterintelligence matrix (Section 8.4)
- Contour 3: Measures and tools of counterintelligence (Section 8.5)
  - Multipurpose nature of counterintelligence measures (Subsection 8.5.1)
  - Physical security (Subsection 8.5.2)
  - Information and technological systems security (Subsection 8.5.3)
  - Personnel security (Subsection 8.5.4)
  - Counterintelligence monitoring, investigation and collection (Subsection 8.5.5)
  - Counterintelligence exploitation, deception and neutralisation (Subsection 8.5.6)

We summarise and conclude the chapter in **Section 8.6**.

8.2 COUNTERINTELLIGENCE – WHY IT IS NEEDED AND IMPORTANT AS A BUILDING BLOCK

In order to explicate CI as a building block of our FCCI, we have to conceptually explain CI in considerably more detail than has thus far been done in this study. A more detailed explanation of CI, which extends beyond a mere demarcation of its interaction with CCI, is required for two reasons:

(1) CCI is interwoven and inseparably linked with the entire multidisciplinary CI effort. In other words, CCI is not a neat compartment within CI. As will be demonstrated in Chapters 10, 11 and 13, CCI involves all the other CI fields.

(2) CCI is modelled on and derives much of its terminology from CI. Phrased differently: applied to the cybersphere, 'traditional' CI theory and practice provide a 'conceptual template' for moulding CCI.

To further explain CI as an FCCI building block, we now discuss the following three contours which we deem essential to describing CI, namely:

- Contour 1: Definition of counterintelligence (Section 8.3)
- Contour 2: Notional structure and principles of counterintelligence (Section 8.4)
- Contour 3: Measures and tools of counterintelligence (Section 8.5)

8.3 CONTOUR 1: DEFINITION OF COUNTERINTELLIGENCE

We commence explaining CI as a building block of our FCCI with a definition of CI as the first contour. To this end, we firstly remark on the contested nature of defining CI (Subsection 8.3.1). We then offer our own working definition (Subsection 8.3.2).

8.3.1 COUNTERINTELLIGENCE AS A CONTESTED CONCEPT

CI is notoriously difficult to define, since it is relevant to so many of an organisation's activities. The following observation by a CI veteran, nearly four decades ago, endures to this day:

> It is not easy, nor can one feel confident, to re-enter this world where, it has been said, the tortuous logic of counterintelligence prevails...Unfortunately, there seems to be no easy way to explain counterintelligence...Because effective counterintelligence is a combination of so many aspects... (Miler 1980)

Part of CI's "torturous logic" is the **ongoing discourse over CI's offensive and defensive dimensions**. Duvenage and von Solms (2013) describe this discourse as follows:

> For some, counterintelligence is all about spies catching and rooting out enemy spies. For others, counterintelligence centres on security measures such as computer passwords, restrictions on the use of computing equipment, security guards, access control and the like. This is also a skewed view. Counterintelligence is both of these aspects and much more.

For the most part, CI is poorly understood even within statutory intelligence structures. This is attested to by an earlier cited observation by Michelle Van Cleave (formerly US national counterintelligence executive):

> [I]ntelligence studies are now part of most serious International Relations departments and are integrated into the curriculum at our nation's war colleges. But the role of counterintelligence remains little known or understood among scholars or practitioners of national security and policymaking. (Van Cleave 2007)

Since it is not well understood by all practitioners in foremost statutory intelligence agencies, the conceptual confusion over CI in the academic and corporate worlds are unsurprising.

In this subsection, we pointed out the difficulty of defining and explaining CI. It is necessary to be cognisant of this because challenges to define and explain CI impact the delineation of CCI and thus the construction of our FCCI.

8.3.2 WORKING DEFINITION OF COUNTERINTELLIGENCE

Recognising these challenges, and although it will inevitably be contested, this thesis requires a **tentative working definition to delineate CI as a building block of our FCCI**. Expanding on earlier contributions (Duvenage & von Solms 2013; Duvenage, Jaquire & von Solms 2016), we thus define CI as follows:

> CI denotes the collective of measures an organisation undertakes to identify, deter, exploit, degrade, neutralise and protect against adversarial intelligence activities and internal risks deemed as detrimental or potentially detrimental to the organisation's vital informational interests and the pursuance thereof.

While the definition captures CI's essence, it can for reasons of brevity not reflect certain key principles which underpins and notionally structure CI. This **notional structuring and assumptions** are important because they impact the way we practice **CI** and **CCI**. A notionally structuring of CI, for example, not only contextualises CCI but also provides the conceptual template (mentioned in Subsection 8.3.1) to mould CCI in Chapters 9-11 and 13.

In this section, we defined CI and highlighted the necessity of notionally structuring CI.

8.4 CONTOUR 2: NOTIONAL STRUCTURING AND PRINCIPLES OF COUNTERINTELLIGENCE

Following on the working definition provided in Subsection 8.3.2, in this section, we show the notional structure of CI by means of a diagram (Figure 23) and explain the principles underpinning the diagram. This is an attempt to explicate "effective counterintelligence" and its "tortuously logic" as plainly as possible (*cf.* Miler 1980).

As a starting point, we provide the following diagram of a notional structure of CI:

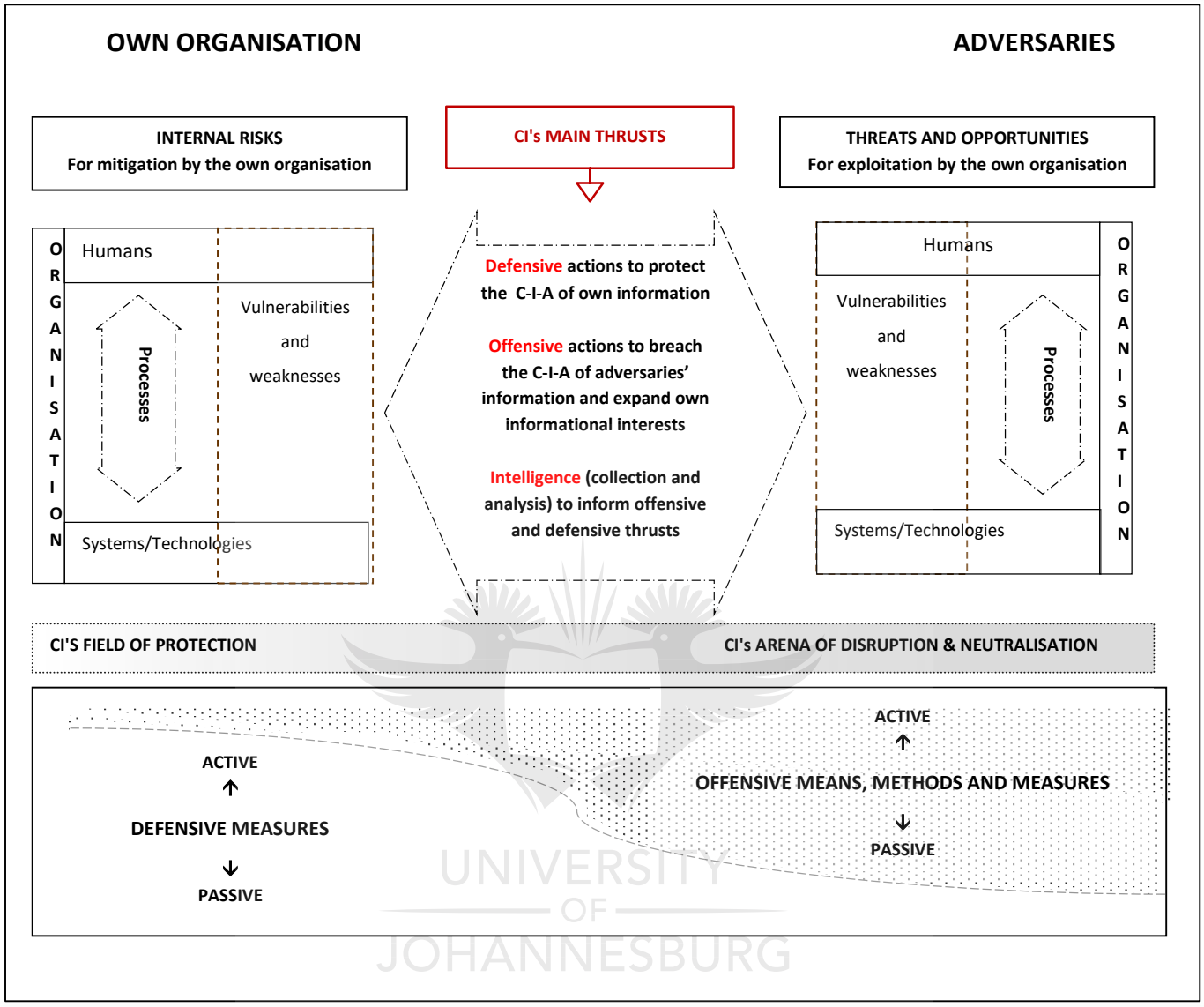


Figure 23: Notional structure of Counterintelligence (adapted from Duvenage 2011 and Duvenage & Hough 2011)

While not exhaustive, there are seven CI principles which underpin and explain Figure 23.[10] The reader shall benefit by looking at Figure 23 after reading each of the following principles (Prunckun 2012; Godson 2001; Duvenage 2011; Duvenage & Hough 2011):

- **Principle 1: CI protects the confidentiality-integrity-availability (C-I-A) of** the own **organisation's vital informational interests**. 'Integrity' here refers to information's veracity and reliability, while 'confidentiality' pertains to guarding

[10] To maintain argumentative logic, the explanation of principles overlap with assertions made earlier in this thesis.

against unauthorised disclosure of information. Availability denotes the effective working of systems, repositories and processes pertaining to such information.

- **Principle 2: Information resides in systems** (including physical records and IT systems), **processes** (such as communication) and **human beings**, and depends on **technologies**. Institutions and individuals are the custodians of information. CI therefore safeguards the relevant institutions, systems, technologies and processes. It also ensures the integrity of human beings who have access to the information.
- **Principle 3**: CI guards against **internal risks** (weaknesses and vulnerabilities) and exploits **external threats** as well as opportunities. The compromising of information through human negligence or insecure systems is an example of an internal risk.
- **Principle 4**: CI seeks to **exploit adversaries by breaching** their informational assets' **C-I-A** and by exploiting their vulnerabilities and weaknesses.
- **Principle 5**: **External threats are posed by adversaries** that seek or attempt to **breach the own organisation's C-I-A**. These adversarial actions assume various forms and can broadly be clustered into espionage (intelligence), aspects of covert action (deception and disinformation), and the disruption or manipulation of information through for example hostile cyber activities. Adversaries include opposing nation states, entities in private enterprise, NGOs, entities in the mass media, terrorist and extremist groupings, and unaffiliated individuals/groups. In contemporary reality, these role-players as well as the clusters of adversarial actions are interwoven in an intricate web.
- **Principle 6: CI's defensive and offensive missions are informed by intelligence[11] (i.e. the collection and analysis of all-source information)**. Some of this information is collected and assessed by CI. Effective CI, however, also benefits in this regard from information provided by the other elements (see Subsection 7.3.2 of Chapter 7). Likewise, CI generates information of value to positive intelligence and covert action. For its part, offensive CI uses aspects of covert action to influence and mislead espionage adversaries. Offensive CI and

[11] 'Intelligence' as used here should not be confused with the 'intelligence' building block (Chapter 7) or 'positive intelligence' (Subsection 7.3.2 of Chapter 7). 'Intelligence' as used here is a general term which denotes collection and analysis to produce actionable information. The use of the term 'intelligence' in the literature is not only ambiguous, but highly contested. For a more detailed clarification on the ambiguous uses of the term, please see Subsection 7.3.2 (Chapter 7) as well as Section 2 in Duvenage, von Solms and Corregedor 2015.

the informational aspects of covert action are in fact sometimes nearly indistinguishable. In all cases, the analysis of collected information is critical. In this regard, Godson (2001) asserts: “Perhaps the queen of the counterintelligence chess board is counterintelligence analysis, both offensive and defensive.”

In what could be confusing, CI is thus deemed to have two primary missions (offense and defence), but three thrusts (offense, defence and intelligence). To clarify this point, with a view to elaborating further in Chapter 9 (Section 9.4), we can tabulate this distinction as follows:

Table 4: Counterintelligence Thrusts and Primary Missions (Author)

	CI Thrusts	**CI Primary Missions**
Offense	✓	✓
Defence	✓	✓
Intelligence	✓	x

- **Principle 7: CI has four modes (postures**) which are executed in accordance with a four-sector matrix. Figure 23 shows both offensive and defensive CI measures, with each having an active and a passive dimension. As a result, CI has four modes, namely passive–defensive, active-–defensive, passive–offensive and active–offensive. Although the interplay offensive–defensive is further explained in Subsection 8.5.1 below, for the purposes of explaining CI principles, we can summarise the four modes as follows:

Table 5: Four-sector Counterintelligence Matrix (adapted from Duvenage & von Solms 2013, as compiled from narratives in Prunckun 2012, Sims 2009 and Godson 2001)

<table>
<tr><th colspan="2">DEFENSIVE MODE
Denies adversaries access to and generates information about adversaries.</th></tr>
<tr><td>Passive Defence
Denies the adversary access to information through physical security measures and other security systems.</td><td>Active Defence
The active collection of information on the adversary to determine its sponsor, modus operandi, network and targets. Methods include physical and electronic surveillance, dangles, double agents, moles and electronic tapping.</td></tr>
<tr><th colspan="2">OFFENSIVE MODE
Primarily aim at manipulating, degrading, controlling and neutralising adversaries. Generates information on adversaries.</th></tr>
<tr><td>Passive Offensive
Reveals to the adversary what you want them to see. This could range from selective exposure of actual information to decoys and dummies. The adversary is thus left to draw its own inferences and interpretations.</td><td>Active Offensive
The adversary is fed with disinformation and its interpretation thereof manipulated. Disinformation can be channelled through for example double agents and ‘moles’.
Active-offensive CI could include some forms of Covert Action. Covert action, in its use here, denotes the targeting of an adversary through the influencing of events, conditions, individuals, groups or institutions to the benefit of a sponsor in a manner not attributable to the sponsor or offering plausible deniability. Influencing is achieved through measures that vary from paramilitary and political actions to propaganda and intelligence assistance.</td></tr>
<tr><td colspan="2">Both passive-offensive and active-offensive modes generate information on adversaries.</td></tr>
</table>

In this section, we notionally structured CI by means of a graphic depiction and discussing its underlying principles. The **notional structuring constitutes Contour 2** of CI as an FCCI building block. In Chapters 9 to 13, this general notional structuring of CI is applied more practically and specifically to CCI. In Chapter 10 (Table 6 and Figure 31), for example, the above matrix is applied to CCI.

We now proceed with examining, as Contour 3 of the FCCI’s CI building block, the clusters of CI measures.

8.5 CONTOUR 3: COUNTERINTELLIGENCE MEASURES AND TOOLS

An examination of CI measures, wider than just those in the cyber realm, is **necessary since these other methods support CCI** (see Chapter 13). Furthermore, and as mentioned earlier, several CCI means and measures are modelled on long-established concepts that include denial, deception, honeypots and double agents.

In our explanation of CI means and methods, we firstly observe the multifunctional nature of CI measures and then proceed to explain the various clusters of CI measures. To this end, this Section is structured as follows:

- Subsection 8.5.1 – Multipurpose nature of counterintelligence measures
- Subsection 8.5.2 – Cluster 1: Physical security
- Subsection 8.5.3 – Cluster 2: Information and technological systems security
- Subsection 8.5.4 – Cluster 3: Personnel security
- Subsection 8.5.5 – Cluster 4: Counterintelligence monitoring, investigation and collection
- Subsection 8.5.6 – Cluster 5: Counterintelligence exploitation, deception and neutralisation

8.5.1 MULTIPURPOSE NATURE OF COUNTERINTELLIGENCE MEASURES

Since it aids conceptualisation and discussion, we typically group CI measures in different clusters such as physical security, information and systems security, personnel security, monitoring, investigation and collection as well as exploitation, deception and neutralisation. From our discussion in Section 8.4, it should be clear that **clusters of CI measures are not watertight compartments serving only one of the defensive, offensive or intelligence CI thrusts**. Measurers deployed defensively can simultaneously provide information and act as triggers to alert the offensive side of CI. Similarly, offensive instruments (e.g. a double agent used for deception) can render information useful to the proactive configuration of defences. Likewise, various measures can be deployed passively and/or actively.

This interplay can be explained by means of the well-known **sword-and-shield** analogy. CI employs measures relatively non-aggressively (the shield) and aggressively (the sword). In combat, the sword and the shield function in synergy (Duvenage & von

Solms 2015, Duvenage 2011). “The shield is primarily designed for defence but in the hand of a master can be used offensively too. Similarly, the sword is an offensive weapon (stab and cut) that can also defend (block) from an attack. Employed against an enemy the sword and shield reveals information on such an adversary's weapons and skills. This information is continuously used to redirect the use of the own sword and shield (Duvenage & von Solms 2015, Duvenage 201).

With the qualification advanced above on the multifunctional nature of CI measures, we will now discuss the various clusters. **The discussion of these clusters builds on, and contain extracts from, previous research by the author (Duvenage 2011, Duvenage 2013)**.

8.5.2 CLUSTER 1: PHYSICAL SECURITY

"Physical security has historically been dominated by “police”-type management, processes and enforcement approaches. This type of physical security relies on a combination of measures, on a lighter note referred to as "gates, guards, guns and dogs" (Francq 2000). Although this police-type function is still required, today’s security vulnerabilities are increasingly technical in nature and related to IT systems, software, and hardware (Taylor 2007).

Physical security is directed towards the facilities where information is produced and stored, as well as the physical safety of infrastructure and equipment to store and relay information. For nation states, the physical security of the whole **national critical informational infrastructure** thus ought to be of the highest concern. For smaller organisations, physical security is narrower in scope and include access and movement control, perimeter security, alarm systems, safes and vaults, fire prevention measures, key control, control of the removal and transfer of information and equipment, and the physical security of the organisational ICT infrastructure (within their control).

8.5.3 CLUSTER 2: INFORMATION AND TECHNOLOGY SYSTEMS SECURITY

As suggested above, there is an overlap and inseparability between 'physical security' and what in this study are termed ‘information and technological systems security’. ‘Systems’, as used in this context, is deemed to refer to a variety of information and communication systems. For ease of reference, we **henceforth** use the acronym **INSYSEC** for **information and technological systems security**.

In our view, the use of the acronym 'INSYSEC' will clarify the confusion caused by the sometimes dogmatic use of long-established terminologies. Such dogmatic conceptualisations are not congruent with the converged reality presented by contemporary practice. Illustrative of the latter is the separation of CI into the distinctive subfunctions of 'information security' (INFOSEC, which is sometimes erroneously deemed synonymous with 'computer security'); 'technical security countermeasures' (TSCMs); communication security (COMSEC) and **cyber security** (**CYBSEC**). Technological advances have blurred the distinction between the security of information (in whatever format) and the security of systems. Communication and information systems are by and large an aggregate. Against this background, **this thesis posits INFOSEC, TSCMs, COMSEC and CYBSEC all as dimensions of INSYSEC**.

As part of INSYSEC, '**information security**' pertains *inter alia* to the classification, distribution and control of access to information and systems. Access to such information will be determined by the level of security clearance an individual has as well as the relevance of the information to his/her line function (Taylor 2007). The latter is usually defined as the need-to-know or compartmentalisation principle (Wettering 2000). Information classification and the need-to-know principle provide parameters according to which personnel are given access to information and computer, communications and other systems.

System security is, however, far more encompassing than mere internal access to systems. In addition to limiting access to authorised users ('confidentiality'), its other two primary goals are the 'integrity' and 'availability' of information/communication systems (Crampton *et al.* 2006). Phrased differently, system security has CI's earlier noted threefold aim, namely to protect against (i) compromising information (unauthorised access to information), (ii) integrity violation (altering information through replacement and manipulation) and (iii) denial of service (which results in systems being wholly or partially incapacitated for the intended users) (Crampton *et al.* 2006). The reasons for the existence of these systems are the storage, processing, retrieval and communication of information. From this line of reasoning, it is clear that COMSEC is an integral part of INSYSEC. In addition to securing cyber systems, COMSEC safeguards other electronic communication instruments. COMSEC thus overlaps with **cyber security (CYBSEC)**. Similarly, TSCM is not – as projected by authors such as Wettering (2000) – a distinct and separate "collection of technical efforts to detect the technical penetrations of facilities by foreign intelligence services to collect intelligence". Resulting from the integration of systems outlined, TSCMs are interwoven with several

dimensions of INSYSEC. For this reason, effective **vulnerability and penetration testing** should gauge the security of INSYSEC in its entirety and not only that of computer systems.

As part of our explanation or discussion of CI measures, in this subsection, we outlined INSYSEC and contextualised CYBSEC. In the next subsection, we focus on personnel security.

8.5.4 CLUSTER 3: PERSONNEL SECURITY

“However well protected by other measures, the fidelity of personnel with actual or potential access to sensitive information and systems remains arguably the most critical factor of CI” (Duvenage 2011). Over decades, the most damaging breaches within statuary intelligence services internationally followed ‘insiders’ volunteering their services to foreign intelligence services, and multiple others involved foreign intelligence services’ recruitment of ‘insiders’ (Duvenage 2011; Taylor 2007). Recently, whistleblowers such as Edward Snowden and Chelsea Manning have illustrated the impact of publicised breaches of information on statutory state security. Numerous other breaches resulted from negligent '**insider**' actions. It is, for example, suspected that the compromising of a US National Security Agency ‘cyber weapons arsenal’ by the Shadow Brokers group in 2016 resulted (at least in part) from an operative’s negligent actions. Currently, 'insiders' – whether intentionally or through negligence – are behind the vast majority of the most severe cyber breaches (IBM 2016).

Pre-employment and in-service personnel security are consequently of self-evident significance. Methods used as part of determining the security competence and suitability of personnel include biographical verification, criminal record checks, lifestyle and financial analysis, interviews and polygraph tests. Simultaneously, awareness programmes (including cybersecurity skilling) are indispensable CI tools. Complementing the latter, **proactive cyber measures** aimed at mitigating the insider threat include decoys, tripwires and honeynets.

In the preceding paragraphs, we examined personnel security as a cluster of CI measures. In the next subsection, the focus is on CI monitoring, investigation and collection as a further cluster of such measures.

8.5.5 CLUSTER 4: COUNTERINTELLIGENCE MONITORING, INVESTIGATION AND COLLECTION

To detect breaches and/or adversarial intelligence activities, CI relies on a range of detection and monitoring measures. Should indications of a breach and/or adversarial intelligence activities be detected, CI would not summarily 'plug the leak'. The further monitoring and investigating of the leak could, for example, expose other undiscovered adversarial espionage agents and networks.

Effective exploitation of 'holes in the fence' presupposes sound information and intelligence. Consequently CI could opt for continued monitoring and the further collection of information through investigation. In such collection, investigation and monitoring, human and technical means are combined.

Surveillance is one of the most common CI collection methods and demonstrates the interaction between technical and human dimensions. Although reality is more complex, three subcategories of surveillance can be distinguished conceptually. These are: (a) static surveillance, (b) mobile surveillance and (c) electronic/digital surveillance (*cf.* Prunckun 2012). Cyber surveillance is an exponential growing subset of electric/digital surveillance. The integration of digital devices in personal lives and contemporary society exponentially increases the reach of cyber surveillance on individuals and organisations. Cyber surveillance includes on-the-network actions. The 'fishbowling' of suspected cyberespionage could for one render invaluable information. A "fishbowl" is described by Mena (2003) as the action to "contain, isolate, and monitor an unauthorized user within a system in order to gain information about the user".

In addition to surveillance, CI monitoring, investigation and collection traditionally relied and will continue to rely on a range of **human sources**. HUMINT sources include, but are not limited to, peripheral agents, agents-in-place, access agents, 'moles', defectors, double agents, multiturned agents (e.g. triple agents), agent *provocateurs*, 'walk-in' agents, agents of influence, witting/unwitting agents, penetration agents, infiltration agents, false-flag agents, 'sleepers' and 'honeypots/ravens'. These different descriptors of sources are not mutually exclusive. Under certain conditions, a human source can for example be typified simultaneously as a mole, a defector and a double agent. If such a person used sexual allure to achieve ends, he/she can also be described as a honeypot (female) or raven (male). These agents can be recruited through the cold, developmental or combined approach, and their utilisation can be witting or unwitting.

Their recruitment and handling can furthermore be done under own, false and combined flag.

Technological advances increasingly facilitate the **acquisition and utilisation of human sources**. The recruitment of human assets on cyber platforms serve as one such example. In addition, technological advances enable the creation and utilisation of 'sock puppets' (fake cyber persona, sometimes automated) which engage with adversarial entities (Lee 2014d; Bardin 2011). Sock puppets and avatars are as varied as conventional human sources and can serve various collection and monitoring purposes. On the one hand, their effectiveness depends on the application of time-tested HUMINT techniques of recruitment and handling. On the other hand, their efficiency is increasingly bolstered by advanced Artificial Intelligence (AI).

It should be emphasised that besides HUMINT and Cyber Intelligence, CI should benefit from the own organisation's collection, also from other technical domains (SIGINT, IMINT and MASINT).

In this subsection, we described CI monitoring, collection and investigation as a cluster of CI measures. In the next subsection, we focus on the CI exploitation, deception and neutralisation cluster of measures.

8.5.6 CLUSTER 5: COUNTERINTELLIGENCE EXPLOITATION, DECEPTION AND NEUTRALISATION

Even if CI monitoring, collection and investigation have extensively and beyond a reasonable doubt identified an adversarial espionage network, a subsequent 'plug of the leak' would still not necessarily be the next step. Instead, the organisation can opt for continued monitoring to be accompanied by the deception of and 'feeding' of disinformation to an adversary. The ultimate prize is influencing the adversary through deception of its intelligence effort and for the benefit of the own organisation. This is fittingly encapsulated in the following observation by Codevilla (1992): "**Action against the enemy through the enemy's own intelligence is the very consummation of CI**." To this end, CI (as noted earlier) uses aspects of informational covert action.

In the case of HUMINT, this deception could be achieved by 'feeding' information to an adversarial espionage network. In a similar manner, misleading information can be relayed through technical channels known to be targeted by an adversary, namely CYBINT, SIGINT, IMINT and MASINT.

Disinformation/denial and deception can also be pursued by means of, for example, double agents or/and agents of influence – be it in the 'real' or digital realms. (The application of such tools within the cyber realm is discussed in Chapters 9-11).

Although neutralisation can partially be accomplished through exploitation and deception, CI operations eventually conclude with a distinctive **neutralisation and termination** phase. This process is described in more detail in Chapter 13 (the CCI process). Suffice to state here that CI termination can either be opted for (at the initiative of the own organisation) or imposed by circumstances. In the case of a nation state, termination can take various forms, such as prosecution, expulsion, public exposure, diplomatic protest and -under certain circumstances- acts of physical harm (including elimination/assassination).

Which form will be opted for ought to balance short-term benefits with longer-term advantages. In this regard, Hulnick (2007) asserts:

> Finally, in the last step of the counterintelligence process, authorities often make public claims of success, a rare step in intelligence work. Normally intelligence managers try hard to keep successes secret so that they might be repeated. An oft-quoted CIA saying is, "The secret of our success is the secret of our success." In cases in which intelligence has been gathered successfully, it is critical to protect sources and methods. In counterintelligence, however, the claim of success, when the case has ended, could be used to convince the public that the government is ever watchful and actually doing something with the billions of dollars spent on intelligence.

Also in the case of organisations other than nation states, the distinctive advantages of termination options should be considered. If executed skilfully, protected termination and neutralisation could provide the 'seeds' for a subsequent 'generation' of CI operations (Duvenage & Hough 2011).

In the preceding section, we outlined the CI measures and found that these measures are as diverse as the threats confronting the organisation. CI was found to be a multidisciplinary endeavour requiring the synergetic employment of measures. In order to aid our discussion, we conceptually clustered the measures. However, in their practical execution, the measures are part of a multifaceted entirety **which constitutes Contour 3 of CI as the fourth building block of our FCCI**.

8.6 CONCLUSION

The discussion of CI measures above formed part of our unpacking of CI as a building block of our FCCI.[12] In advancing this building block, we discussed three contours essential to demarcating CI, namely: (1) a definition of CI, (2) discussion of CI's notional structuring and principles, and (3) discussion of CI methods. Throughout the discussion, it was clear that CI in the cybersphere is inextricably interwoven with CI in other fields. Moreover, in the rest of this thesis, effective CCI will be shown as being modelled on CI.

In the next chapter, we present CCI as a further building block of our FCCI.

[12]This chapter is based on, and contains verbatim extracts from Duvenage 2011; Duvenage & Hough 2011; Duvenage 2013; Duvenage & von Solms 2014; Duvenage, von Solms & Corregedor 2015.

CHAPTER 9

BUILDING BLOCK 5 – CYBER COUNTERINTELLIGENCE

9.1 INTRODUCTION

In the preceding chapter (Chapter 8), we forwarded CI as Building Block 4 of our FCCI. We positioned CCI as part of the broader multidisciplinary CI endeavour (see Section 8.5 of Chapter 8). In this chapter, the focus is on explicating the central and defining building block of our FCCI, namely CCI. We do this by defining and describing CCI with specific reference to the wide array of tools available to CCI. The addition of CCI as Building Block 5 of our FCCI can be illustrated as follows:

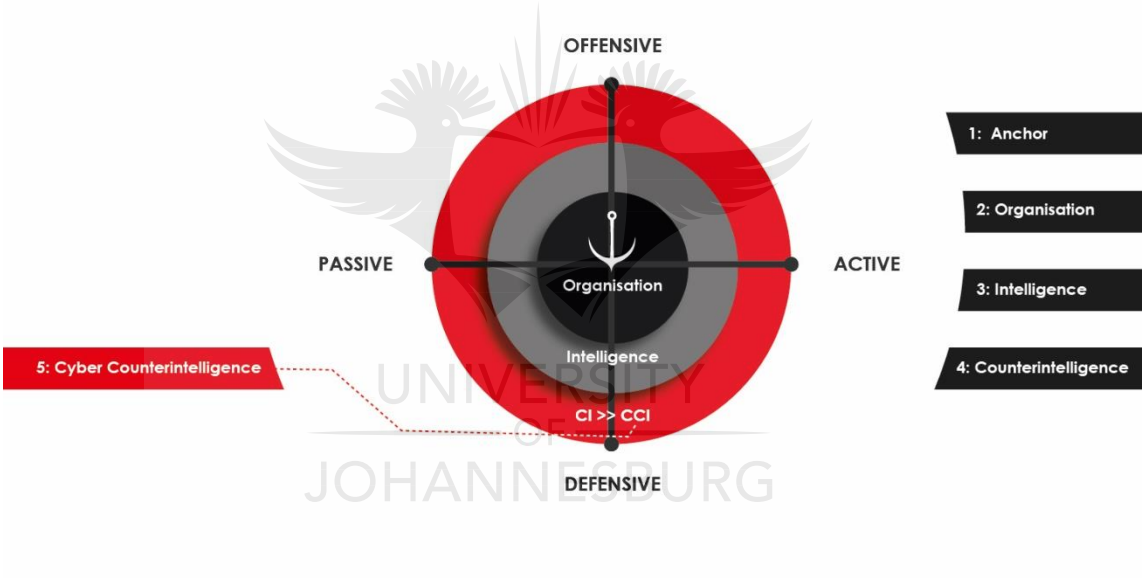


Figure 24: Building Block 5 – Cyber Counterintelligence (Duvenage, Sithole & von Solms 2017)

To explain CCI as Building Block 5 of the FCCI, the rest of this chapter is structured as follows:

- Section 9.2: Cyber Counterintelligence– Why it is needed and important as a building block
- Section 9.3: Defining Cyber Counterintelligence
- Section 9.4: Cursory overview of Cyber Counterintelligence tools
- Section 9.5: Conclusion

9.2 CYBER COUNTERINTELLIGENCE – WHY IT IS NEEDED AND IMPORTANT AS A BUILDING BLOCK

To illustrate the interlock between CI and CCI, the preceding diagram (Figure 24) deliberately depicts CI and CCI in the same 'ring' and on the same level. This is done to graphically reflect this thesis's recurring theme, namely that CCI is but a tool type within the broader CI toolset. As is clear from the term "**cyber** counterintelligence", this building block of our FCCI explicates CCI as a predominantly – but not exclusively – technical toolset "relating to, or involving computers or computer networks" (Merriam-Webster 2017).

While intrinsically linked with broader CI, CCI is thus a distinctive specialisation field. This distinctive specialisation field is the essential descriptor and defining element of a CONCEPTUAL **FCCI**. Phrased differently, we cannot have a conceptual FCCI without **CCI** as a central building block. Consequently, the importance of CCI as a building block of the FCCI is self-evident and its importance can hardly be overemphasised.

In this section, we discussed the need for and importance of CCI as a building block of our FCCI. In the next section, we commence our description of this building block by examining some existing definitions of CCI and offering our own definition.

9.3 DEFINITION OF CYBER COUNTERINTELLIGENCE

As suggested in the last paragraph of the preceding section, a description of CCI ought logically to start with a definition of CCI. One of the earliest definitions of CCI found for this study was advanced by the US Department of Defence (US 2001) which described CCI as "[m]easures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions".

This definition is useful in that it qualifies CCI as pertaining to (a) the adversarial use of cyber means and (b) the adversarial targeting of cyber assets also through other traditional methods (HUMINT and TECHINT). Given the multiplicity of hostile cyber actors, in our view CCI can however not be limited to "foreign intelligence services".

Recognising threat actors other than foreign intelligence services, Carroll (2009) describes CCI as:

> …all efforts made by one intelligence organization to prevent adversaries, enemy *intelligence* organizations or *criminal* organizations from gathering and collecting sensitive digital information or intelligence about them via computers, networks and associated equipment. CCI are measures to identify, penetrate, or neutralize computer operations that use cyber weapons as a means and mechanism to collect information. (emphasis added)

What the above, and other definitions of CCI in the literature we consulted, lack is categorically linking CCI with multidisciplinary CI. Therefore, and building on our earlier contributions (Duvenage & von Solms, 2014; Duvenage, von Solms & Corregedor 2015), this thesis **defines CCI as the subset of multidisciplinary CI aimed at detecting, deterring, preventing, degrading, exploiting and neutralising adversarial attempts to collect, alter or in any other way breach the C-I-A of valued information assets through cyber means**.

In this section, we concisely overviewed some definitions of CCI and concluded by forwarding our own definition. In the next section, we explain CCI in more practical terms by discussing some standards, technologies, tactics, measures and procedures.

9.4 CURSORY OVERVIEW OF CYBER COUNTERINTELLIGENCE TOOLS

9.4.1 INTRODUCTION AND APPROACH

The CCI toolset comprises an extensive range of standards/guidelines/frameworks, technologies, tools, tactics, measures, techniques and procedures. In the interest of simplicity, in this thesis, **'tools'** will henceforth be used as a **generic term** referring to the collective of 'standards/guidelines/frameworks', 'technologies', 'tools', 'tactics', 'measures', 'techniques' and 'procedures'. However, in cases where more specificity is required, the pertinent applicable term (e.g. ‘techniques’ when referring to 'cryptanalysis', 'binary obfuscation', 'click jacking', etc.) will be used.

Most of the tools are not unique to CCI. What is unique, within the context of this thesis, is their application in combination with other CI tools – and in a manner best achieving CI’s three main thrusts of **defence**, **offense** and **intelligence** (i.e. the collection and analysis of information). These main CI thrusts were discussed in Chapter 8 (Section 8.4, Principle 6), graphically illustrated in Figures 23 and Table 4 (Chapter 8), and are thus not further elaborated on here.

CCI's pursuance of these three main thrusts incorporates tools, models and approaches advanced in the fields of 'Active Cyber Defence' and 'Cyber Denial and Deception'. This synergy is, for example, illustrated by Stech and Heckman's (2018) 'Cyber Counterintelligence Framework in Active Defense' and Fieber's (2015) 'Organizational CI Process Model' - both of which are discussed later on (in Chapters 10 and 13 respectively).

It is important to reiterate that the aim of this thesis is to advance a conceptual framework and not a manual for CCI work. Consequently, a detailed discussion of CCI tools falls outside the focus of this thesis. As stated in Chapter 2 (Subsection 2.2.2), our emphasis is rather on providing a skeletal structure which can on the one hand systemise existing knowledge and on the other hand direct further academic enquiry. Accordingly, this section provides a cursory overview of CCI tools in a manner useful to the conceptual structuring of CCI. To this end, the rest of the Subsection is structured as follows:

- Subsection 9.4.2: Cyber counterintelligence tools – Defensive thrust
- Subsection 9.4.3: Cyber counterintelligence tools – Offensive thrust
- Subsection 9.4.4: Cyber counterintelligence tools – Intelligence thrust
- Subsection 9.4.5: Basic taxonomy of cyber counterintelligence tools

9.4.2 CYBER COUNTERINTELLIGENCE TOOLS: DEFENSIVE THRUST

The defensive end of the CCI tools spectrum is typically premised on cybersecurity standards, guidelines and frameworks prescribed by transnational institutions, governmental bodies and industry. Duvenage, Sithole and von Solms (2017) cite as examples those prescribed in/by the National Institute of Standards and Technology, Control Objectives for Information and Related Technologies, International Organization for Standardization (ISO), Information Technology Infrastructure Library, International Society for Automation, International Electro-technical Commission, Web Application Security Project and Federal Financial Institutions Examination Council. Serving as further illustration are the guidelines advanced per the US Department of Defence's Security Technical Implementation Guides as well as the technical-security configuration guides of the US National Security Agency and similar bodies (Duvenage, Sithole & von Solms 2017).

As the FCCI's predominantly technical toolset, the CCI building block (and the subsequent blocks discussed in Chapters 10 to 13) has to be configured with **due**

consideration of – but also distinctly **move beyond** – these cybersecurity standards, guidelines and frameworks. Flowing from these standards, guidelines and frameworks, tools associated with CCI's defensive thrust pertain to physical defensive, personnel/user defensive and system defensive techniques (see ① in Figure 28, pages 107-108. These tools thus overlap substantially with three clusters of CI tools described in Chapter 8 (Section 8.5), namely: physical security (Cluster 1), IT systems security (Cluster 2) and personnel security (Cluster 3). Emphasising the IT systems security cluster, Jaquire (2018) cites the following as examples of specific defensive CCI techniques:

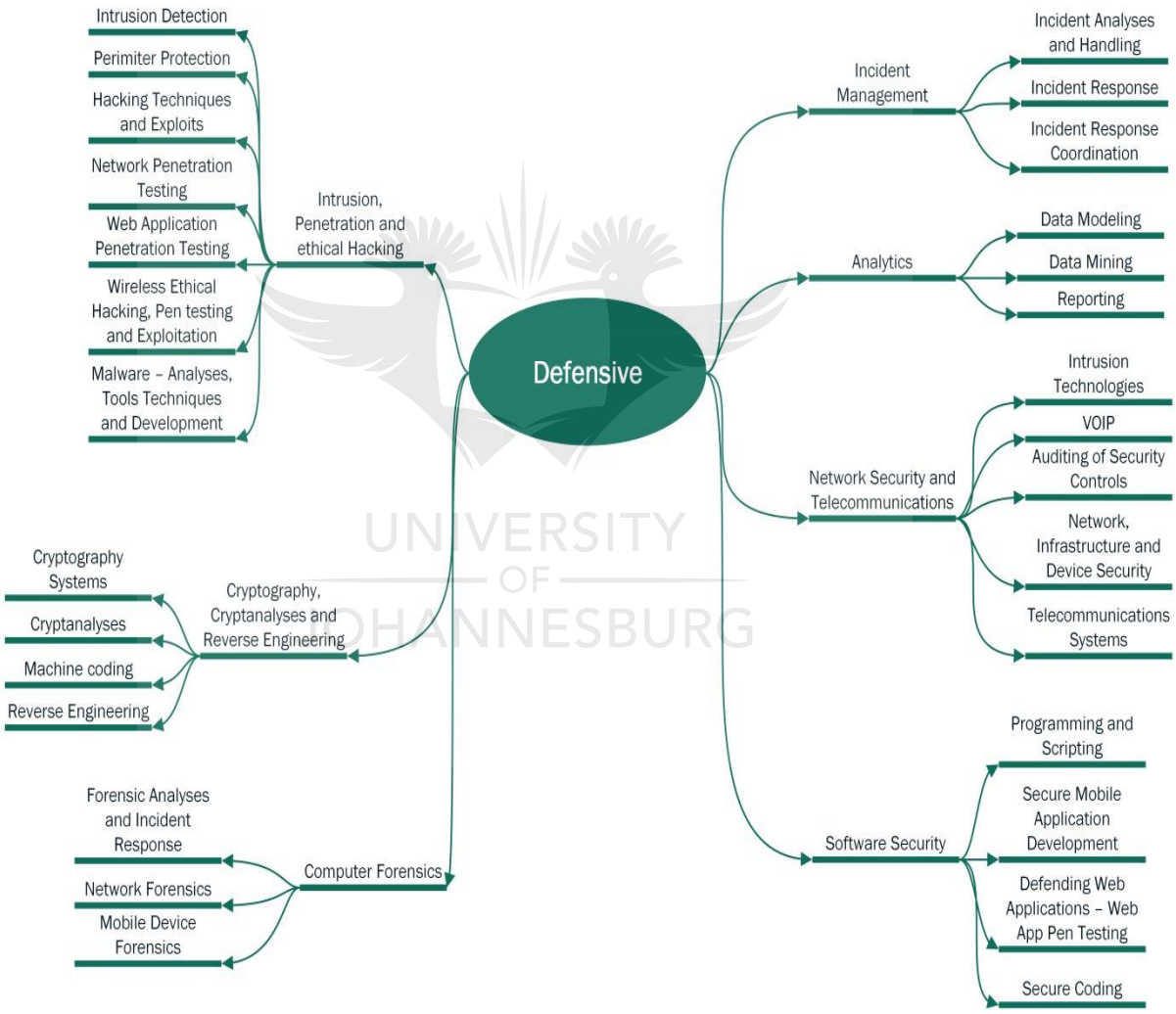


Figure 25: A Non-comprehensive Illustration of Defensive CCI Techniques (adapted from Jaquire 2018)

In this subsection, we discussed the defensive thrust of CCI**.** This **defensive thrust** is depicted in Figure 28 as ① (pages 107-108). We now proceed with outlining CCI's offensive thrust.

9.4.3 CYBER COUNTERINTELLIGENCE TOOLS: OFFENSIVE THRUST

CCI's offensive thrust comprises various tools and actions that actively target and exploit opponents' systems. Offensive CCI tools thus forms part of CI Cluster 4 (CI monitoring, investigation and collection) and CI Cluster 5 (CI exploitation, deception and neutralisation). These clusters were discussed in Chapter 8 under Sections 8.5.5 and 8.5.6. Examples of CCI tools deployed offensively are mentioned in Figure 28 (pages 107-108) in the columns under the heading **Offensive Thrust** (marked as ②). Complementary to the tools mentioned in Figure 26, Jaquire (2018) cites Heckman *et al.* (2012) and illustrates offensive CCI with reference to the following techniques:

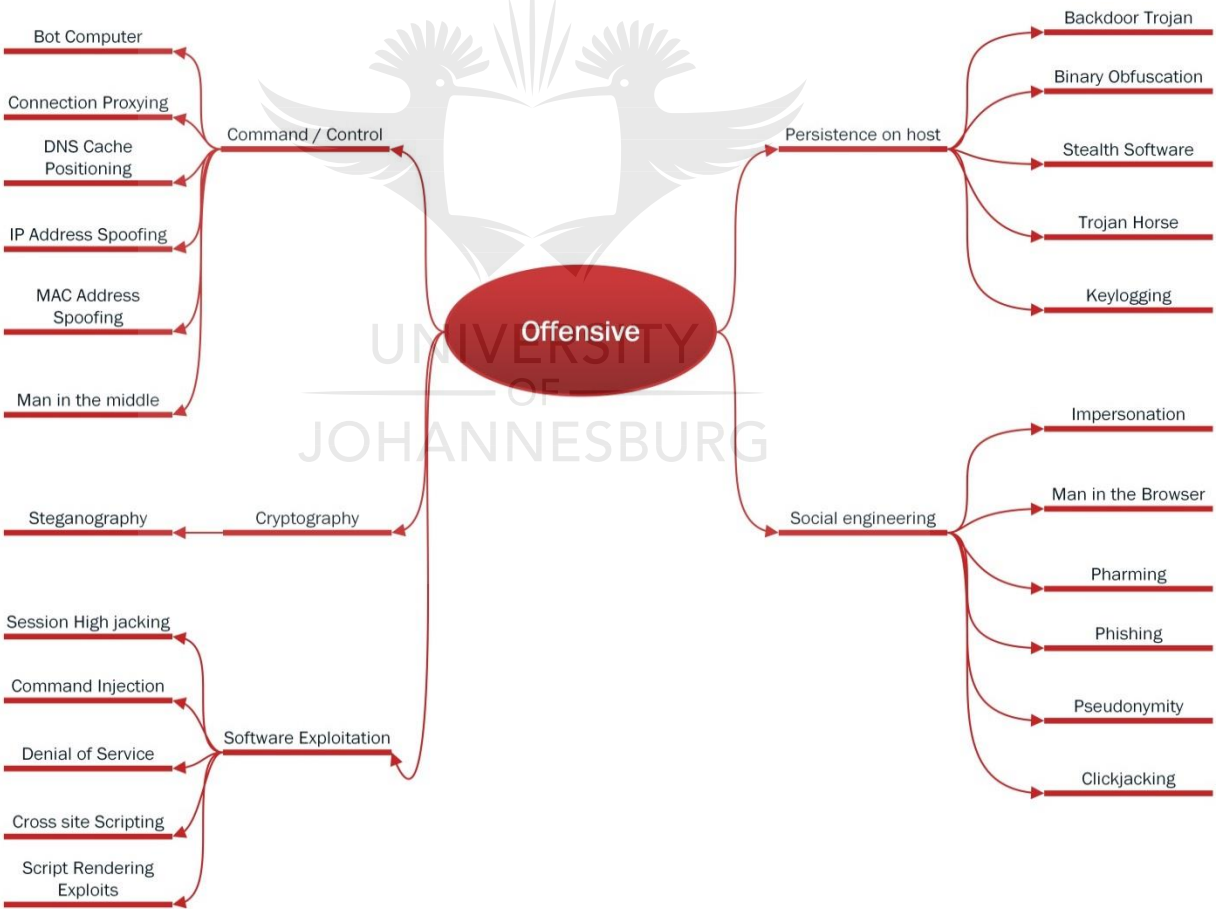


Figure 26: Non-comprehensive Illustration of Offensive CCI Techniques (adapted from Jaquire 2018, Heckman et al. 2012)

In line with the multipurpose nature of CI measures in general (Subsection 8.5.1 of Chapter 8), and CCI, these tools can mostly not be compartmentalised as serving only the offensive thrust. They can, in part, also be defensive. The sword-and-shield analogy explained earlier (Subsection 8.5.1 of Chapter 8) in relation to CI measures generally therefore applies to CCI tools. With reference to CCI techniques, Jaquire (2017) selectively illustrates this overlap as follows:

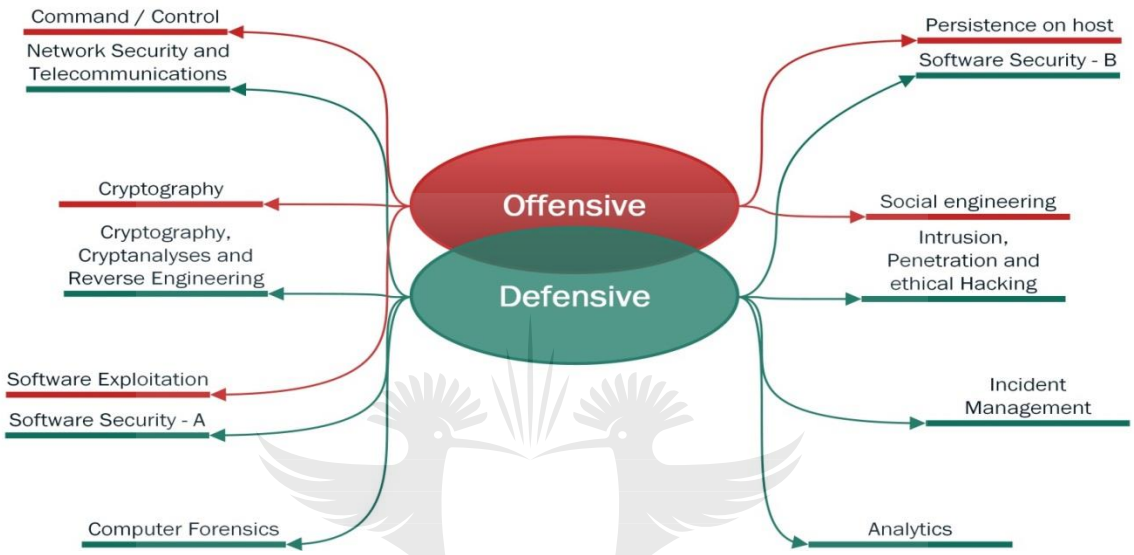


Figure 27: Non-comprehensive Illustration of the Overlap between Offensive and Defensive CCI Techniques (adapted from Jaquire 2018)

9.4.4 CYBER COUNTERINTELLIGENCE TOOLS: INTELLIGENCE THRUST

Whether deployed defensively and/or offensively, CCI tools are also used to collect data and information which are analysed to produce actionable intelligence. In this respect, these tools thus serve CCI's intelligence thrust.[13] This is depicted in Figure 28 (pages 107 -108) which shows the **Intelligence Thrust** as marked ③.

In addition to, and often overlapping with defensive and offensive tools, there has of late been an explosion in the market of products and services specifically aimed at providing "intelligence" of various kinds (Duvenage, Jaquire & von Solms 2016). Threat intelligence in particular has evolved in a “catchall term for a vast array of different technologies, methodologies and ideas” (Schoeman 2015). Depending on the vendor,

[13] 'Intelligence' as used here should not be confused with the 'intelligence' building block (Chapter 7) or 'positive intelligence' (Subsection 7.3.2 of Chapter 7). 'Intelligence' as used here is a general term which denotes collection and analysis to produce actionable information.

threat intelligence can denote one or more of feed-, research- and platform-driven products (Schoeman 2015). For some 'threat intelligence' is just relabelled anti-virus signatures at a much higher cost, while for others it means an overarching approach central to an organisation's strategy (Duvenage, Jaquire & von Solms 2016). Similar to other technical tools, threat intelligence technologies and methodologies should form part of a balanced CCI approach. For a more detailed discussion on the relationship between CCI and threat intelligence, see Annexure E (Duvenage, Jaquire & von Solms 2016).

In the preceding subsections (9.4.2–9.4.4), we discussed CCI tools from the perspective of the offensive, defensive and intelligence thrusts. In the next subsection, we propose a basic taxonomy which accommodates these three thrusts in an integrated postulation on CCI-relevant tools.

9.4.5 BASIC TAXONOMY OF CYBER COUNTERINTELLIGENCE TOOLS

The nature of a taxonomy of CCI tools is self-evidently influenced by the level of appraisal. For reasons discussed in the introduction (Subsection 9.4.1), we took a high-level approach in compiling a basic taxonomy of CCI tools. In addition to being qualified as basic, the taxonomy does not purport to be comprehensive or exhaustive, but rather it is illustrative. It should be emphasised that **Artificial Intelligence (AI)** is increasingly central to various tools and is thus not discussed separately within the taxonomy's subsets. With these caveats, the taxonomy advanced in this thesis is as follows:

Please turn to the next two pages for Figure 28.

<table>
<tr><th colspan="3">. ① DEFENSIVE THRUST</th></tr>
<tr><td colspan="3">Passive ⟷ Active</td></tr>
<tr><td colspan="3">Deny Detect Collect & Analyse (③Intelligence Thrust)</td></tr>
<tr><td colspan="3">Standards, guidelines and frameworks</td></tr>
<tr><td>Physical Defensive</td><td>Personnel/User Defensive</td><td>System Defensive</td></tr>
<tr><td>Protects against:
• Unauthorised access to facilities and systems
• In loco theft of data, hardware
• Introduction of malware through physical access to systems
• Unauthorised altering or destruction of data
• Physical destruction or access denial
• Unauthorised reading (acoustic, visual, radiation, analogue, signals)
• While not conventionally seen as a Physical Defence, supply-chain management has a physical defensive function. It is also part of System Defences as an enabler.</td><td>Consists of aspects such as:
• IT and user personnel vetting, re-vetting, confidentiality agreements and monitoring
• Personnel security measures, BYOD user parameters or exclusions
• User programmes in cyber security that cover policy and procedures for the handling of security-related incidents, malfunctions and recovery.
• Overlapping with system defences, the use of software decoys and traps to mitigate the insider threat
• Investigations focussed on cyber security incidents involving personnel. Could also include digital forensic investigations.</td><td>Comprises a combination of:
• Hardware and software such as:
✓ Network perimeter-based security (filters, certain firewalls, IDS and IPS etc.)
✓ Malware scanners.
✓ Integrated automated systems/tools (that collect and evaluate information about devices connected to a network, activities thereon – inclusive of intrusions). Examples of such tools, discussed further on in the Figure are decoys, honeypots and behavioural analyses toolsets.
✓ Overlapping with the latter, depending on its configuration, a honeynet can be defensive or offensive in type/mode. The term fish bowling denotes the defensive configuration.
• Processes (such as supply-chain management are also in part system defences).
• Vulnerability assessments, penetration testing and verification testing (on products, systems, software and secure code).
• Incident and threat monitoring, identification, investigation and response. A CERT is per definition defensive – although it might contain offensive elements in its responsive action.
• Port level security and BYOD regulation in as far as network interfacing is concerned (Also part of Personnel Defences).</td></tr>
<tr><td></td><td colspan="2">• Commercial Cyber Threat Intelligence products, services and platforms.
• Analysis of data and information and through automated and human means.</td></tr>
<tr><td rowspan="2"></td><td colspan="2">• The use of software decoys to mitigate the insider threat is an overlap between personnel and system defensive measures. They are mostly active CCI means.</td></tr>
<tr><td>• Investigations focussed on internal cyber security incidents involving personnel. May include digital forensic investigations.</td><td>• Investigations of external cyber intrusions could be part passive and part active system defence.</td></tr>
</table>

<table>
<tr><th colspan="3">②OFFENSIVE THRUST</th></tr>
<tr><td colspan="3">Passive ⟷ Active</td></tr>
<tr><td>Collect & Analyse (③Intelligence Thrust)</td><td>Disrupt Exploit</td><td>Destroy</td></tr>
<tr><td>• Collection of information on and the monitoring/surveillance of the cyber sphere to detect cyber adversaries and their exploitation of the cyber sphere in a manner that is not own-network restricted – (i.e. requires more than deployment of systems described under defensive mode). Could, depending on configuration also include IDS/IPS, honey-client applications (as opposed to host-based honeypots), luring and some forms of data mining.
• The recruitment and handling of virtual agents on underground forums (true or false flag) that can serve the purpose of enticement, collection and/or exploitation. (Some ‘virtual’ agents can also develop into HUMINT assets).
• Analysis of information and data through automated and human means.</td><td>Measures taken to exploit and neutralise adversaries activities in the cyber sphere:

• System and honeynet configured offensively with the aim of enticing, exploiting and deceiving adversaries. False information is displayed to adversarial reconnaissance tools, network scanners and listeners, etc. This has as one of its aims to lead adversaries in the direction of your own preference.
• Tarpits and black holes.
• Utilisation of virtual agents for offensive purposes.</td><td>Cyber warfare, in the full extent of the term, is typically excluded from the mandate of civilian intelligence communities. A cyber warfare capability should be flexible and allow utilisation without, or in conjunction with, kinetic war.

Nevertheless, a top class civilian CCI outfit will need to have the authority and capacity to very selectively conduct operations that have cyber warfare characteristics, utilising cyberwarfare- related techniques. Such cyber CCI operations will share characteristics with covert action. (Covert action aims to influence role-players, conditions and events without revealing the sponsors identity.)

Within business, the use of offensive measures will be determined by the legislative and regulatory framework within which the entity operates.</td></tr>
<tr><td colspan="3">Cyberespionage on adversaries. Distinguishable from own-system collection (IPS, IDS, honeynets etc) on the basis that adversarial networks are targeted actively and exploited in accordance with strategic and operational objectives.</td></tr>
</table>

Figure 28: Basic Taxonomy of CCI Tools (adapted from Duvenage, von Solms & Corregedor 2015

It would have been noticed that the taxonomy in Figure 28 also provides for a **passive–active** range in respect of both the defensive and offensive thrusts. This range is indicated in both instances with **purple font** and a two-pointed **purple arrow (←→)**. As a perusal of the taxonomy in Figure 28 will confirm, tools at the active end of the spectrum are, in comparison to passive tools, decidedly more 'aggressive' and involve the active engagement of adversaries. The interplay between passive-active and defensive-offensive tools is further discussed in the next chapters (Chapters 10-11).

9.5 CONCLUSION

In this chapter, we advanced and described CCI as a building block of our FCCI. We defined CCI and gave a high-level overview of CCI tools with reference to CCI's offensive, defensive and intelligence thrusts. This high-level overview was consolidated into a taxonomy. In the next chapter, we add the CCI matrix as a further FCCI building block.

CHAPTER 10

BUILDING BLOCK 6.1 – CYBER COUNTERINTELLIGENCE MATRIX: HORIZONTAL PLANE

10.1 INTRODUCTION

In Chapter 9, we posited CCI as the fifth building block of our FCCI. Moving from this, this chapter forwards a CCI matrix as the sixth building block of our FCCI. We show that this matrix is crucial to academically explaining and practically executing CCI.

It will be recalled that an offensive-defensive matrix has partially been explained in a broader counterintelligence context in Chapter 8 (Section 8.4, Figure 23). In this chapter (Chapter 10) we expand and apply this matrix to the cyber sphere. Graphically, the addition of this matrix as Building Block 6 of our FCCI looks like this:

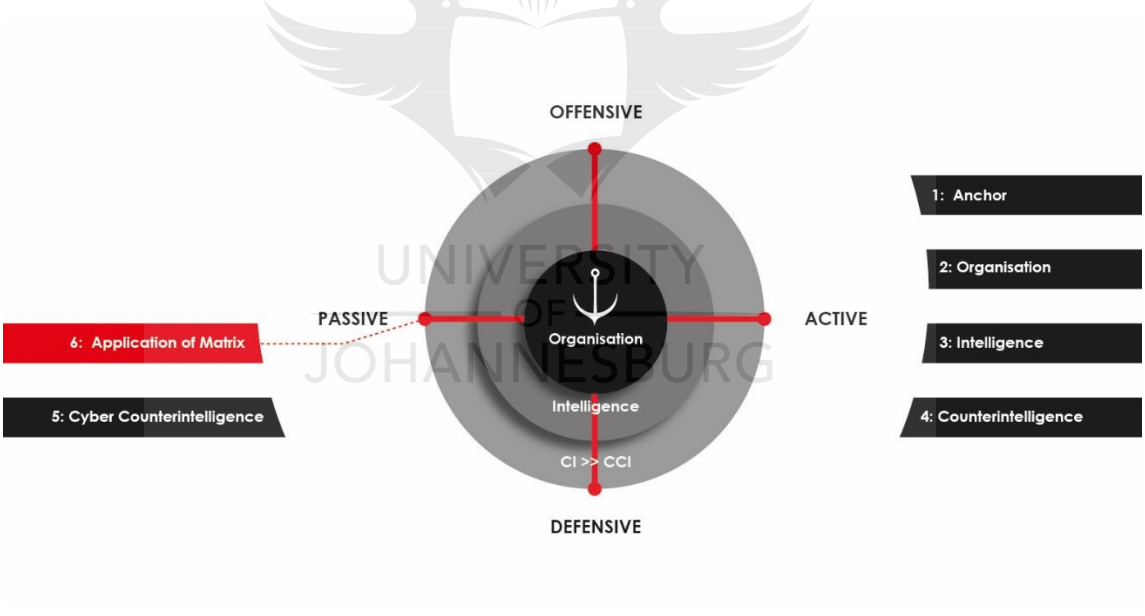


Figure 29: Building Block 6 – Application of the CCI Matrix (Duvenage, Sithole & von Solms 2017)

To facilitate to an easier reading experience, we divided the design of the CCI matrix in two chapters. Chapter 10 explains the CCI matrix's composition and its horizontal plane, while Chapter 11 presents the matrix's vertical plane. Since it consists of both a vertical and a horizontal plane, the **CCI matrix is a three-dimensional construct**. This is further explained in Section 10.3.

Chapter 10 and Chapter 11 are in part based on - and contain verbal extracts from Duvenage, Jaquire and von Solms (2019). This paper accompanies the thesis as Annexure K.

The rest of Chapter 10 is structured as follows:

- Section 10.2: Cyber counterintelligence matrix – Why it is needed and important as a building block
- Section 10.3: Overview of the cyber counterintelligence matrix's composition
- Section 10.4: Matrix's horizontal plane – Cyber counterintelligence modes
    - Subsection 10.4.1: Recapitulating the Four-Sector Counterintelligence Matrix
    - Subsection 10.4.2: Application of the CI Matrix to CCI
    - Subsection 10.4.3: The CCI Matrix in Practice – A Hypothetical Case Study
- Section 10.5: Conclusion

10.2 CCI MATRIX – WHY IT IS NEEDED AND IMPORTANT AS A BUILDING BLOCK

Thus far, it is clear to the reader that CCI is intricate and complex. Consequently, CCI's conceptual structuring and practical execution pose several challenges. Of these, the following interrelated challenges are pertinent to this chapter:

- How can the wide array of CCI tools (Section 9.4 of Chapter 9) be optimally utilised and synchronised with other CI measures (Section 8.5 of Chapter 8)?
- How can CCI be integrated and aligned with the broader organisational intelligence and CI endeavour on all the different organisational layers?
- How does CCI's execution on the different organisational layers differ and how are they related?
- Seeing that the organisation is the FCCI's pivot (Section 6.1 of Chapter 6), what notional aid can be forwarded to assist in best configuring its CCI posture in accordance with its interests, goals and strategy (Figure 16 in Chapter 6 and Figure 20 in Chapter 7)?

As suggested above, a conceptual 'solution' to the above challenges is of both practical and academic importance. Therefore, our FCCI should have, as one of its building blocks, a notional construct that meets these challenges. (See Subsection 2.2.4 of

Chapter 2 for the FCCI's criteria.) We advance the CCI matrix as this notional construct and as the sixth building block of our FCCI.

10.3 OVERVIEW OF THE MATRIX'S COMPOSITION

This building block consists of the CCI matrix, which has a vertical and horizontal plane. Graphically depicted, the **three-dimensional CCI matrix** is as follows:

Figure 30: CCI Matrix (Author)

The CCI matrix's **horizontal** plane depicts the four quadrants which represent the CCI posture's four modes, namely:

(1) Passive-defensive
(2) Active-defensive
(3) Active-offensive
(4) Passive-offensive

The matrix's **vertical** plane (i.e. Figure 30's three layers) integrates CCI with the broader organisational, intelligence and CI endeavour at the various levels on which CCI functions. This is done by describing CCI's execution on three organisational levels/layers, namely:

(1) Strategic
(2) Operational
(3) Tactical/Technical

In this section, we briefly outlined the composition of the CCI matrix. In the next section, the CCI matrix's horizontal plane is explained in more detail.

10.4 HORIZONTAL PLANE OF THE MATRIX: CYBER COUNTERINTELLIGENCE MODES

The explication of the matrix's horizontal plane consists of:

- Subsection 10.4.1: Recapitulating the four-sector counterintelligence matrix
- Subsection 10.4.2: Application of the counterintelligence matrix to cyber counterintelligence
- Subsection 10.4.3: The CCI matrix in practice – a hypothetical case study

10.4.1 RECAPITULATING THE FOUR-SECTOR COUNTERINTELLIGENCE MATRIX

In our discussion of both CI tools generally (Section 8.5 of Chapter 8) and CCI specifically (Section 9.4 of Chapter 9), we firstly noted that tools can be used for defensive and/or offensive purposes. Secondly, we asserted that both offensive and defensive tools can be deployed passively and/or actively. Flowing from these two assertions, we derived four modes for classifying CI and CCI tools, namely: passive–defensive, active-defensive, passive-offensive and active-offensive.[14] In doing so, we applied CI's Principle 7 (which holds that "CI has four modes which are executed in accordance with a four-sector matrix") to the CCI environment. This principle was discussed in Chapter 8 (Section 8.4) and explained by means of the following table (next page):

[14] These four modes were shown in Chapter 8 (Table 5) as the four quadrants of the CI matrix. For our purpose here, 'quadrants' and 'modes' are identical and the terms are thus used interchangeably.

Table 5: Four-sector Counterintelligence Matrix (Author)

<table>
<tr><th colspan="2">DEFENSIVE MODE
Denies adversaries access to and generates information about adversaries.</th></tr>
<tr><td>Passive Defence
Denies the adversary access to information through physical security measures and other security systems.</td><td>Active Defence
The active collection of information on the adversary to determine its sponsor, modus operandi, network and targets. Methods include physical and electronic surveillance, dangles, double agents, moles and electronic tapping.</td></tr>
<tr><th colspan="2">OFFENSIVE MODE
Primarily aim at manipulating, degrading, controlling and neutralising adversaries. Generates information on adversaries.</th></tr>
<tr><td>Passive Offensive
Reveals to the adversary what you want them to see. This could range from selective exposure of actual information to decoys and dummies. The adversary is thus left to draw its own inferences and interpretations.</td><td>Active Offensive
The adversary is fed with disinformation and its interpretation thereof manipulated. Disinformation can be channelled through for example double agents and ‘moles’.
Active-offensive CI could include some forms of Covert Action. Covert action, in its use here, denotes the targeting of an adversary through the influencing of events, conditions, individuals, groups or institutions to the benefit of a sponsor in a manner not attributable to the sponsor or offering plausible deniability. Influencing is achieved through measures that vary from paramilitary and political actions to propaganda and intelligence assistance.</td></tr>
<tr><td colspan="2">Both passive-offensive and active-offensive modes generate information on adversaries.</td></tr>
</table>

10.4.2 APPLICATION OF THE COUNTERINTELLIGENCE MATRIX TO CYBER COUNTERINTELLIGENCE

The four-sector CI matrix is applicable to the full spectrum of CCI tools. At the one end of the spectrum, conventional intrusion prevention systems (IPS)/intrusion detection systems (IDS) serve as examples of passive–defensive tools. At the other end of the spectrum, a cyber weapon designed to destroy, disrupt or manipulate an opponent's systems constitutes an active-offensive tool. CCI tools can seldom be pigeonholed as having only a defensive or offensive purpose, or as being either active or passive. For the most part, to reiterate one of this study's recurring emphases, tools are useful to two or more of the four modes. A honeynet, for example, can be used passive-

offensively (e.g. to feed disinformation to an adversary) and active-defensively (e.g. to collect information on an opponent). Graphically, this can be depicted as follows:

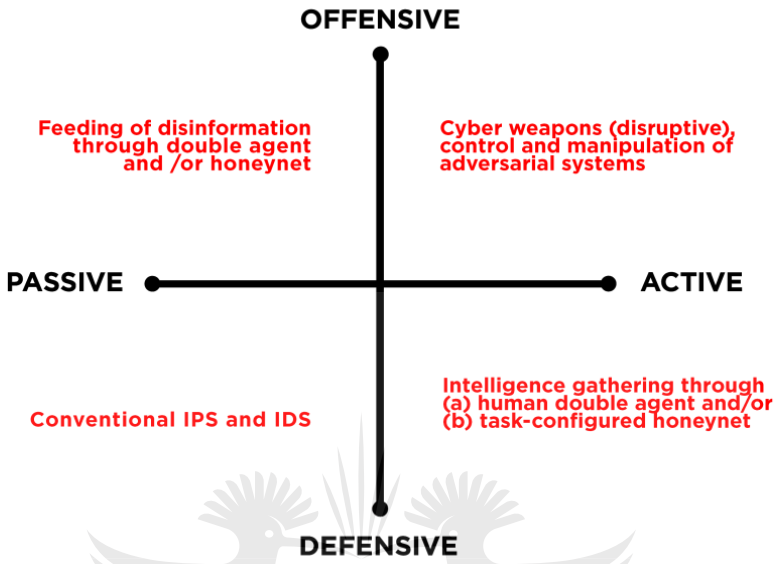


Figure 31: Some CCI Tools Plotted on the CCI Matrix's Horizontal Plane (Author)

As an academic construct, Figure 31 is useful for the categorisation of CCI tools and to explain their relationship with CI tools in fields other than the cyber field. In CCI practice, Figure 31 could have the following three uses:

(1) **Ensure each CCI tool is utilised to maximum effect**. Since most tools can have more than one purpose, they should be measured against the CCI matrix with the question 'In addition to its initially intended role, in what other modes can the tool be used?' Figure 31, for example, depicts a honeynet deployed in both the active-defensive and passive-offensive modes. To expand on the example used in Figure 31. A honeynet can (if required and depending on circumstances) also be used to facilitate hacking back and the deployment of cyber weapons (active-offensive). If otherwise configured, a honeynet could furthermore be deployed in tandem with IDS/IPS (passive-defensive). In this hypothetical example, a honeynet is therefore relevant to all four modes.

(2) **Synchronise CCI tools/actions with other CI tools/actions**. The plotting of CCI and other CI tools/actions in Figure 31 will aid the synchronisation of efforts and thus optimise the effectiveness and integration of the CI efforts. The feeding of disinformation through a human agent, to use the example depicted in Figure 31

(passive-offensive mode), should be congruent with disinformation 'planted' in an organisation's honeynet. Incongruences between these two 'feeds' of disinformation could comprise both CI HUMINT and CCI operations. Similarly, the CCI matrix can be utilised to plot and synchronise CCI tools and actions with those in other TECHINT areas (see Table 3, Taxonomy of Technical Intelligence Fields, in Chapter 7).

(3) **Configure the CCI posture in accordance with the type and needs of a specific organisation**. In Chapter 6 (Sections 6.2 and 6.3) and Chapter 7, we showed CCI's *raison d'être* to be an organisation's interests, goals and strategy (IGS). Consequently, the organisation's IGS will ultimately determine the configuration of the CCI posture. Statutory military and intelligence services, for example, will typically have a substantial amount of resources directed to the active-offensive mode. The same will not be the case in relation to, for example, a NGO involved in humanitarian aid. Figure 31 can accordingly be used as a template for plotting and appropriately configuring an organisation's CCI posture. (For a more detailed application of the CCI matrix in configuring an organisation's CCI posture, **please see Figure 3 in Annexure K** on **page 327** of the thesis).

10.4.3 THE CCI MATRIX IN PRACTICE – A HYPOTHETICAL CASE STUDY

As will be discussed in the more detail in the next Section (10.5), the configuration of the organisation's CCI posture on the strategic (interests, goals and strategy) and operational levels shapes CCI activities on the tactical-technical level. This point, as well as the application of our CCI matrix, are illustrated by Stech and Heckman's (2018) proposition on a "Cyber Counterintelligence Framework in Active Defense". Utilising a hypothetical case study of a NATO CCI campaign against "advanced persistent threat actors associated with Russia, known as APT28 and APT29", Stech and Heckman (2018) pose the following as NATO's strategic CCI goal and operational objectives:

- "Support NATO strategic deception goal: convince Russian authorities their cyber intelligence supports propaganda but is not ready for kinetic war against NATO;
- Active & Passive CCI Defense: Reduce and eliminate effectiveness of APT28 tactics, techniques, and procedures for espionage; Eliminate or counter APT28 and APT29 malware and tradecraft;
- Passive CCI Offense: Poison APT28 and APT29 intelligence stream with deception materials; eliminate, corrupt, or covertly take over control of attackers' command and control; and

- Active CCI Offense: Feed Russian espionage units with false information (e.g. feed APT29 false information about actions and effects of APT28, and *vice versa*).
- Support apparent intrusion successes with cyber and non-cyber strategic NATO deception operations."

In extending the strategic goal and operational objectives to the tactical-technical level, Stech and Heckman (2018) apply our four-sector matrix – advanced earlier in this thesis per Table 5 and Figure 31) – as follows:

Table 6: Hypothetical NATO Cyber CI Operations against cyber espionage threat (Stech & Heckman 2018)

<table>
<tr><td>Modes</td><td>Passive Cyber CI</td><td>Active Cyber CI</td></tr>
<tr><td rowspan="5">Defensive mode</td><td colspan="2">Deny access and collect on espionage threat</td></tr>
<tr><td>Passive defense:</td><td>Active defense:</td></tr>
<tr><td rowspan="2">Harden endpoint and server configurations</td><td>Gather intelligence on on-going intrusions</td></tr>
<tr><td rowspan="2">Use honeypots to gather late-stage implants and unpatched exploits</td></tr>
<tr><td>Share actionable indicators across NATO intelligence partners</td></tr>
<tr><td rowspan="5">Offensive Mode</td><td colspan="2">Manipulate, degrade, control and neutralize espionage threat</td></tr>
<tr><td>Passive offensive:</td><td>Active offensive:</td></tr>
<tr><td rowspan="2">Use honeypots to deliver deception materials</td><td>Counter-hack hop points and control servers</td></tr>
<tr><td rowspan="2">Trolling "bait victims" to lure attackers to controlled boxes</td></tr>
<tr><td>Sinkhole APT28 hop points</td></tr>
<tr><td>Identify APT28 operatives</td><td>Operating controlled boxes as double agents to inject beacons, double-hacked backdoors, etc. into APT28 control environment</td></tr>
</table>

The hypothetical case study provides a high-level illustration of the CCI matrix's (Table 5) application in guiding an integrated and coherent CCI operation. The application and implications of the matrix are discussed in more detail in Annexure K (pages 322 – 330).

10.5 CONCLUSION

In this chapter, we explained the CCI matrix's horizontal plane and illustrated three applications thereof. While the CCI's matrix's four modes are based on a time-tested CI principle (Chapter 8, Section 8.4 – Principle 7), in this chapter we further developed the concept for application to CCI and imposed the four-mode quadrant as the horizontal plane of the FCCI's matrix. Subsequently, we illustrated the application of our four-mode matrix by citing Stech & Heckman's (2018) hypothetical NATO case study. We mentioned the four-mode matrix's application on the strategic, operational and tactical-technical levels. The next chapter presents these three levels as the CCI matrix's vertical plane.

CHAPTER 11

BUILDING BLOCK 6.2 – CYBER COUNTERINTELLIGENCE MATRIX: VERTICAL PLANE

11.1 INTRODUCTION

In Chapter 10 we explained the CCI matrix's composition and its horizontal plane. In this chapter we advance the CCI matrix's vertical plane. The CCI matrix's vertical plane explains the various levels on which CCI functions and integrates CCI with the broader organisational intelligence and CI endeavour. As was the case with the development of the horizontal plane, we based our design of the vertical plane on an established intelligence study notion, namely the three levels/layers of execution (strategic, operational and tactical/technical).

11.2 APPROACH AND PREMISE

Effective CCI is not only multifaceted but also stratified (Duvenage, Jaquire & von Solms 2016). To be optimal, CCI has to involve all organisational layers, from the C-suite to line functionaries (Duvenage, Jaquire & von Solms 2016). The levels conventionally ascribed to statutory intelligence (namely strategic, operational and tactical) provide a useful approach for also explaining CCI (see Subsection 7.3.3.2 of Chapter 7). These levels are described comprehensively in literature dealing with cyber intelligence/security and cyber threat intelligence. Such works of note include those by Mattern (*et al.* 2014), Friedman and Bouchard (2015), Chismon and Ruks (2015), as well as a series of papers compiled by the Intelligence and National Security Alliance (INSA 2011, 2013, 2014a, 2014b, 2015). We could, however, find no reference in these works to CCI levels.

Although the cited works do not refer to CCI, they partially informed the tabulated synopsis of CCI's levels of execution below (Table 7). These works were also used for the subsequent narrative description of the CCI levels (Sections 11.5.2–11.5.4).

The tabulated synopsis, which provides a reference point and premise for the rest of the chapter, can be depicted as follows:

Table 7: Synopsis of the Levels of CCI Execution (adapted from Duvenage, Jaquire & von Solms 2016)

	Strategic ①	Operational ②	Tactical/Technical ③
CI mission	• Advance and protect organisational interests through defence against and the offensive engagement of adversarial intelligence activities. This is achieved through the following functions: detect, deny, deter, deceive, degrade and/or disrupt.		
CCI mission	• As above, when the adversary uses cyber as a conduit or a cyber asset as a target.		
Leadership	• C-level	• Senior and middle management	• Line and team leaders
Interface with CI	• Organisational, intelligence and CI strategies • All-source CI feed	• Multidisciplinary programmes and operations	• Multidisciplinary projects and continuous line-functional interaction
Referent objects	• Organisation's 'crown jewels' • Critical information and cyber-assets sought (e.g. adversary's 'crown jewels') • Conditions (competitive advantage)	• People, processes, systems, procedures (personal security, ICT architecture and supply-chain management) • Own intelligence programme	• Systems, networks and devices • Network operations • Security operation • CIA (confidentiality, integrity and availability)
Interrogatives	• Who, why?	• Who, where, when, how?	• What, how?
Level of adversarial role-player on which CCI focuses	• Sponsors, opponents and Intelligence capacity	• Intelligence structures, groups and campaigns	• Individuals, TTPs, incidents and actions (on-the-network)
Indicators of targeting and compromise	• Geo-political, sector/industry 'flags' • Analogous events • Adversarial strategy and business decisions	• Operational disruption • Organisational and/or revenue decline • Information leakage	• Breach in the C-I-A of cyber and/or information security milieu • Identification of malicious code, intrusion and threat exploitation
Analysis output	• High-level, strategic appraisals • Strategic warning and advisories	• Operational reports (CCI operations, threat, damage and vulnerability assessments, alerts and warnings) • Trend analyses	• Tactical and technical information reports • Alerts and warnings
Tools – means, methods and measures (offensive, defensive & collection)	• Multidiscipline CI • Strategic direction of means, methods and measures	• As in Figure 28: A basic taxonomy of CCI tools (Chapter 9) • Interlocked with operational and tactical CI	

	Strategic ①	Operational ②	Tactical/Technical ③
Cyber threat intelligence (sourced)	• White papers, non-commissioned and non-commissioned research	• Platforms	• Data feeds
Skill sets required (line-functional)	• Sound knowledge of business and industry • Specialised knowledge and skills in intelligence, multidisciplinary CI and CCI • Strategic analysis and management	• Multi-disciplinary CI • CCI operational and/or technical specialisation • Operational management • Elements of both strategic and tactical	• ICT and information security • Systems, software development, scripting and programming • CCI and CCI technical specialisation • Ethical hacking • Technical cyber defence and collection • Humanities, social sciences and languages • HUMINT • Engineering and reverse engineering

Table 7 cannot be discussed in detail in the confines of a thesis chapter. Therefore, the subsequent sections (11.5.2–11.5.4) do not rigidly mirror Table 7 but are rather aimed at narratively explaining CCI levels in broad terms.

In this section, we introduced the vertical plane of the CCI matrix. This plane consists of CCI levels of execution. To guide our further discussion, we then provided a tabulated synopsis of the different levels of CCI (Table 7). Starting with the strategic level, we now proceed with discussing each of these levels. This discussion is in part based on, and contains verbal extracts from, Duvenage, Jaquire & von Solms 2016.

11.3 CYBER COUNTERINTELLIGENCE ON THE STRATEGIC LEVEL (①IN TABLE 7)

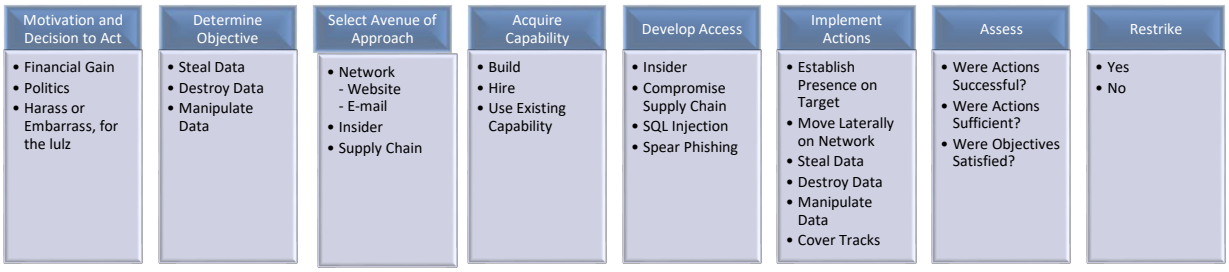
In his benchmark work on CI, Prunckun (2012) rightly asserts that "executive responsibility" is the "first and highest tenant" of CI. For CCI to be successful, the organisation's executive management (C-suite) will have to understand and sanction CCI's missions to advance and protect organisational interests through defence against the exploitation of adversarial, cyber-related intelligence activities (*cf.* INSA 2014b, Chismon & Ruks 2015). Practically, the C-level executive assigned with leading the CI aspect will be responsible for also directing the CCI effort. The executive's responsibilities include obtaining the collective executive management's approval of CCI strategy, priorities, resourcing (funding, infrastructure, equipment, human

resources, skills development/acquisition, etc.). In some instances, the executive would selectively also seek endorsement – normally from the chief executive officer – for high-risk and high-cost programmes. The actual CCI work on a strategic level will be performed by a team consisting of seasoned CCI specialists, multidisciplinary CI specialists, strategic analysts (business and CI) and various other experts relevant to the organisation's core business. To ensure a synergetic approach, some of these specialists and experts will be representatives from the operational CCI level.

CCI informs the C-suite mainly through high-level products and presentations that include estimates, threat and risk assessments, and advisories. These products are informed by appraisal all-source CI operational reports as well as an extensive all-source scanning of the macro-environment for CCI-relevant trends and drivers that could affect the organisation (INSA 2014b). External CTI products sourced would mainly be White Papers as well as commissioned and non-commissioned research papers (Chismon & Ruks 2015). A thorough knowledge of organisational strategy and planning is imperative, as is a clear grasp of the organisation's information-related assets critical for it to exist and prosper – commonly referred to as the 'crown jewels' (INSA 2014b). It is these assets that CCI protects from adversarial intelligence activities and it is the organisational strategy that CCI should advance through the exploitation of adversaries in the cybersphere.

Strategic CCI differs from that on the operational and tactical level in that it takes a wider view of the macro-environment and a longer term view of the actual or potential emergence of threats (Bodmer *et al.* 2012; Mattern *et al.* 2014). Strategic CCI would for instance identify intelligence principals/sponsors that have plausible motive, intent and capacity to target the own organisation through cyber means. In respect of adversarial progression, strategic CCI is thus focused on the first phase of adversarial progression, namely "Motivation and Decision to Act" (see Figure 32).

Figure 32: Adversarial Pathway to an Attack (INSA 2013)



It is important to note that the intelligence principals or sponsors will not necessarily execute the actual intelligence activities but they are the ultimate benefactors (such as a nation state). The actual implementers of hostile cyber as well as associated tactics are those that carry out the task of operational and tactical CCI. While the implementers will determine the operational and tactical avenue of approach, the strategic decisions (e.g. to pursue objectives by human and/or technical means) in this regard will be taken by the intelligence principal.

Strategic CCI is furthermore tasked with detecting high-level indicators that the organisation is being targeted or has been compromised. The focus in this regard is *inter alia* on competitors' business decisions, products launched and markets entered. Similarly, strategic CCI should identify drivers and trends suggesting a rise in the risk of internal compromise (insider threat). Equally important is the detection that organisational strategy and decision making are unduly influenced by deceptive, adversarial cyber operations. Strategic CCI will advise on countermeasures to best exploit adversarial cyber activities to the benefit of the organisation. To be successful, cyber counterdeception and exploitation have to be fully synchronised with such actions in other CI fields (such as agent and double agents operations). Therefore, it is imperative that CCI ensures that countermeasures are aligned with CI and organisational strategy (INSA 2014b). The insights CCI provides are not only of value to the C-level; they are critical to direct actions on the operational and tactical levels. The design and filling of honeypots on the operational and tactical levels, for example, will ultimately be informed by strategic CCI decisions on the nature and direction of counterdeception (*cf.* Bodmer *et al.* 2012).

In this subsection, we discussed the execution of CCI on the strategic level. To recapitulate, this was done since the strategic level is part of the CCI matrix's vertical plane (see Figure 30). We now proceed with describing CCI on the operational level.

11.4 CYBER COUNTERINTELLIGENCE ON THE OPERATIONAL LEVEL (② IN TABLE 7)

As on the strategic level, CCI on the operational level pursues CCI's central missions of defensively and offensively advancing CI-relevant interests in the cybersphere. Adherence to the missions at all three levels ensures a coherent approach and an optimised CCI effort.

Operational CCI is driven by senior and middle management as well as by specialists in the field of CCI operations and analysis. It functions as a conduit and advisory to C-level leadership in matters such as CCI strategic objectives, financials, financial projections and other resource requirements, projects, statistics and reporting. Operational leadership is responsible, among others, for the following main functions (INSA 2014a; Mattern *et al.* 2014):

- Operationalise the CCI strategy as set jointly by the executive management, operational management and CCI experts.
- Develop and implement CCI structures and acquire resources.
- Develop and implement operational plans and identify focus areas.
- Drive daily operations and ensure performance.

Operational CCI is responsible for safeguarding the people, processes, procedures and systems in which the organisation's critical cyber-related assets reside. Consequently, it includes a wide spectrum of organisational functions such as personal security, physical security, procurement, supply chain management, ICT-user management and much more. In addition to conducting CCI operations against adversaries (discussed below), it safeguards the organisation's own information and cyber intelligence operations. It provides operational cyber counterintelligence reports on operations, cyber threats and threat actors, damage and vulnerabilities (as identified through assessments), alerts, warnings and trends to strategic CCI, line-functional managers, analysts and CCI specialist (Riley 2015). It also self-analyses the reports' output with a view to driving reports' outcomes to action (INSA 2013, 2014a).

Operational CCI interfaces with the larger CI function through multidisciplinary programmes and operations, specifically focusing on the cyber part of CI. Its main concern pertains to who the adversaries are; their location or the place from where they operate; their timelines; and their capabilities (such as the ability to utilise or develop malware), intentions (either pronounced or unpronounced) and modus operandi (Chismon & Ruks 2015). Together with this, it is concerned with the adversaries' intelligence structures and their intelligence campaigns (either planned or existing).

With regard to a traditional defensive approach, CCI also focuses on a proactive and reactive function to identify indicators of targeting and compromise (emanating from the cyber field). These are indicators such as a disruption in the organisational operations, organisational decline or a decline in organisational revenue, and/or information leakage. From a reactive perspective, it focuses on these indicators of change and acts

accordingly to counter such instances by identifying its origin and addressing the compromise (by either defensive or offensive means). From a proactive approach, it identifies such possible capabilities and campaigns and addresses threats (by either defensive or offensive means) (Farchi 2012; Bardin 2011).

Operational CCI is persistently seeking exploitable opportunities presented by adversarial cyber campaigns, operations and actions. Through counteroperations, these opportunities are pursued either proactively or reactively – depending on the circumstances.

The skill sets required to capacitate operational CCI are multidisciplinary and include elements such as general management, advanced operational management, CCI analysis, cybersecurity, cyberdefence and offensive CCI techniques, and other fields of technical expertise (Bodmer *et al.* 2012).

In this subsection, we explained the execution of CCI on the operational level. This was done as part of describing the CCI matrix's vertical plane (see Figure 30 and Table 7). Moving from the operational level, we now progress to detailing CCI on the tactical/technical level.

11.5 CYBER COUNTERINTELLIGENCE ON THE TACTICAL AND TECHNICAL LEVELS (③ IN TABLE 7)

Tactical and technical CCI is aimed at achieving the organisation's CCI missions by tactical and technical means. It is driven and executed by line-functional leadership as well as team leaders, role leaders, CCI technical and tactical experts, security analysts and other technical personnel. It has an advisory responsibility to both the operational and executive management that includes matters such as CCI threats and opportunities, defensive and offensive measures, systems and toolsets, CCI analyses and financials (Riley 2015; INSA 2013, 2015). This advisory responsibility is usually fulfilled by submitting tactical products to the operational and, in some instances, directly to the strategic CCI level. Prior to submission to the executive, tactical CCI inputs are normally contextualised at the operational and strategic levels. (For ease of reading, and unless otherwise stated, the term '**tactical CCI**' in the rest of this subsection **refers to both tactical and technical CCI**).

Tactical CCI is responsible, among others, for the following main functions (INSA 2015; Lee 2014b):

- Concretise operational direction into action.

- Identify, design and implement systems, toolsets and reporting mechanisms (both defensive and offensive).
- Carry out tactical taskings in line with CCI operational objectives, through combined technical and HUMINT measures.
- Identify, analyse and action CCI threats and opportunities.

Tactical CCI involves the daily management, configuration (including identification and/or compromise in the case of offensive measure implementation) of both defensive and offensive systems, networks, devices, network operations and security operations (INSA 2015). It is aimed at ensuring the confidentiality, integrity and availability of the organisation's cyber and information security environment, as a defensive tactic and measure. In the case of an offensive or exploit tactics (that must be congruent with operational objectives and the organisational strategy), tactical CCI strives to degrade the confidentiality, integrity and/or availability of an adversary's cyber and information security environment.

It interfaces with the larger CI function through multidisciplinary projects and continuous line-functional interaction. Tactical and operational CCI have a shared focus on on-the-network threats and/or opportunities, threat actors' capabilities or possible capabilities, as well as the deployment and expansion of capabilities. Tactical CCI is concerned with engaging individual groups or individuals, their specific network actions, specific tactics, techniques and procedures, and specific technical issues such as malware signatures (Chismon & Ruks 2015).

Tactical CCI processes feed into information reports and focus on specific issues such as breaches, the identification and/or creation of malicious code, intrusion, threat and exploitation. The process leads to the compilation of tactical and technical reports, alerts, warnings, defensive and offensive solution and action reports, campaign proposals, analyses and interpretations. These are provided to CCI analysts, tactical leadership, operational leadership and the executive in the manner described above (Friedman & Bouchard 2015).

The skill sets required for tactical CCI are, as is the case with strategic and operational CCI, multidisciplinary. They include elements of tactical and line-functional management, ICT security, development of systems and software, programming, scripting, developing offensive and defensive toolsets, CCI technical specialisation, HUMINT and intelligence collection, as well as language and social science expertise (used in, for example, the penetration of hacking forums), ethical hacking, technical

defensive and offensive measures, as well as reverse engineering (Bodmer *et al.* 2012).

In this section, we explicated the execution of CCI on the tactical and technical levels. This was done as part of the description of the CCI matrix's vertical plane and followed on a description of CCI on the strategic and operational levels. We now proceed with summarising and concluding this chapter.

11.6 CONCLUSION

In Chapters 10 and 11, we advanced the sixth building block of our FCCI (namely a CCI matrix comprising two planes). We demonstrated the CCI matrix as essential to explaining and optimising *inter alia*:

- The use and synchronisation of CCI tools
- CCI's levels of execution
- The integration of CCI with the organisational intelligence and CI endeavour
- The configuration of an organisation's CCI posture

In the next chapter, we propose delineation as the penultimate building block of our FCCI.

CHAPTER 12

BUILDING BLOCK 7 – DELINEATION

12.1 INTRODUCTION

In the previous chapter, we described the CCI matrix as Building Block 6 of our FCCI. In this chapter, we forward our FCCI's seventh and penultimate building block, namely delineation. The following aspects are addressed:

- Section 12.2: Delineation – Why it is needed and important as a building block.
- Section 12.3: Some building block contours
  - Subsection 12.3.1: Contour 1 – Delineation of cyber counterintelligence in practice
  - Subsection 12.3.2: Contour 2 – Delineating cyber counterintelligence as a multifaceted academic field
- Section 12.4: Conclusion

Graphically, the addition of delineation as an FFCI building block can be illustrated as follows:

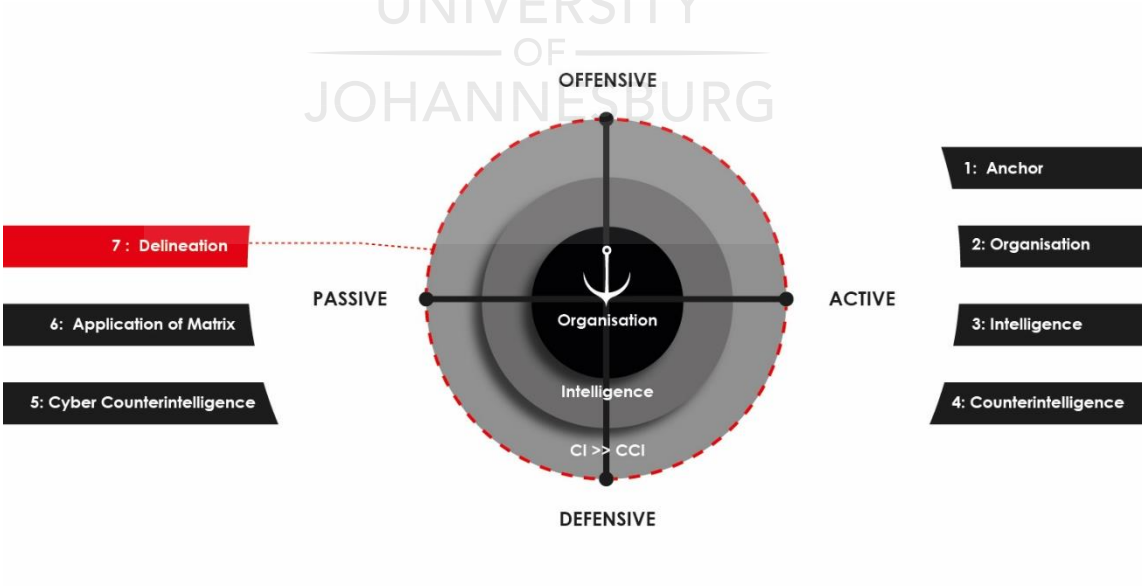


Figure 33: Building Block 7 – Delineation (Duvenage, Sithole & von Solms 2017)

12.2 DELINEATION – WHY IT IS NEEDED AND IMPORTANT AS A BUILDING BLOCK

By its very nature, the cybersphere is one of interconnected reality. Even with all the previous building blocks in place, an organisation would seldom be able – or legally allowed –in **practice to** execute the whole of the CCI endeavour on its own (Duvenage, Sithole & von Solms 2017). Business entities would, for example, be legally prohibited and generally not have the resources to undertake some active-offensive cyber campaigns undertaken by nation states. In a similar vein, a nation state could be necessitated to cooperate not only with other nation states but also with non-state actors in order to achieve national goals. These goals could compel cooperation on CCI. Consequently, and although ultimately driven by each actor's self-centred interests (see Section 6.2 of Chapter 6), effective CCI requires cooperation with other actors and a delineation of respective roles.

Delineation is also important in the **academic** context. Treating CCI as a too wide and encompassing field will result in loss of focus (Duvenage, Sithole & von Solms 2017). Simultaneously, CCI must be clear on its overlaps with various other academic fields and on the areas of multidisciplinary research.

12.3 SOME BUILDING BLOCK CONTOURS

Of all the FCCI's building blocks, the design of delineation is described as the most cursory, and admittedly requires much further research and refinement. Accordingly, in Chapter 15 (Section 15.5), we pose delineation as a priority item on the future research agenda. In this chapter, we make observations about the design of the delineation building block by means of two contours. In line with the distinction drawn in Section 12.2, we structure these contours as pertaining to CCI in **practice** and CCI in the **academic** sphere.

12.3.1 CONTOUR 1 – DELINEATION OF CYBER COUNTERINTELLIGENCE IN PRACTICE

In respect of CCI practice, the delineation building block typically consists of a narrative description of areas of responsibilities and cooperation (Duvenage, Sithole & von Solms 2017). As far as we could ascertain, there are no specific description of CCI responsibility demarcation in **international** agreements between nation states in multinational bodies (such as NATO, the European Union or the African Union). There

are, however, various agreements and other documentation on cooperation in respect of security (including military and combating crime) and cybersecurity. Consequently, the delineation of CCI on an interstate level will be derived from a deductive appraisal of such agreements and documents. Since CCI's signature role is the countering of cyber espionage, international law and convention applicable to the latter should of course also be duly considered. In this regard, the *Tallinn Manual'*s rule 66 on "cyber espionage" is of particular relevance (Schmitt 2013).

In as far as the role of the state in CCI within a particular **nation state** is concerned (i.e. nationally), the legislation, governance frameworks, regulatory stipulations and executive directives of that country need to be considered. Should CCI not be mentioned by name, the demarcation of CCI responsibilities will be derived from the legislation, regulatory stipulations and executive directives on CI. Since CCI is a relatively new field, the demarcation of respective CCI functions and functioning also within specific arms of the state's apparatus and/or in the arena where it operates, would often not be defined in detail. This assertion, as well as the value of conceptual constructs to clarify CCI roles, is capably illustrated by Justiniano's (2017) earlier mentioned master's project entitled 'Advancing the capacity of a theater special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone.'

Legislation, regulatory stipulations and executive directives will be decisive in also demarcating the nature and extent of CCI functions of **non-state actors** within a particular country. In certain respects, the country's state security apparatus could be partially reliant on the cooperation of non-state actors. Simultaneously, and as was noted in the introduction (Section 12.2), non-state actors could be legally prohibited and not have the resources to undertake some active-offensive cyber campaigns. In this regard Fieber (2015) states:

> While private organizations may certainly apply counterintelligence principles with the scope of their operations, legal authorities may limit the extent to which organizations may directly affect an external threat. In that light, close coordination and collaboration ... [with the applicable state security structures] ... are highly recommended

In the case of multinational non-state actors cooperation is more complex and delineation could vary from jurisdiction to jurisdiction.

In this subsection, we examined the delineation of CCI in practice. We now proceed with discussing delineation within the academic context.

12.3.2 CONTOUR 2: DELINEATING CYBER COUNTERINTELLIGENCE AS A MULTI-FACETTED ACADEMIC FIELD

Throughout the thesis, we highlighted CCI as a multifaceted and drawing on several academic fields. These include: Intelligence Studies and International Relations (both part of Political Science), Computer Science, Informatics, Business Studies, Law, Knowledge Management, Sociology, Forensic Science, Psychology, History and Linguistics. Being the multidisciplinary field that it is, CCI cannot be rigidly demarcated. Rather, it is a mosaic of overlapping academic interests. A principle challenge in establishing CCI as an academic field lies in identifying, describing and examining these overlaps.

12.4 CONCLUSION

In this chapter, we explained delineation as an FCCI building block. In the next chapter, we discuss the FCCI's last building block – the CCI process.

CHAPTER 13

BUILDING BLOCK 8 – CYBER COUNTERINTELLIGENCE PROCESS

13.1 INTRODUCTION AND APPROACH

In this chapter, we submit the CCI process as our FCCI's last building block. The addition of the CCI process building block can be depicted as follows:

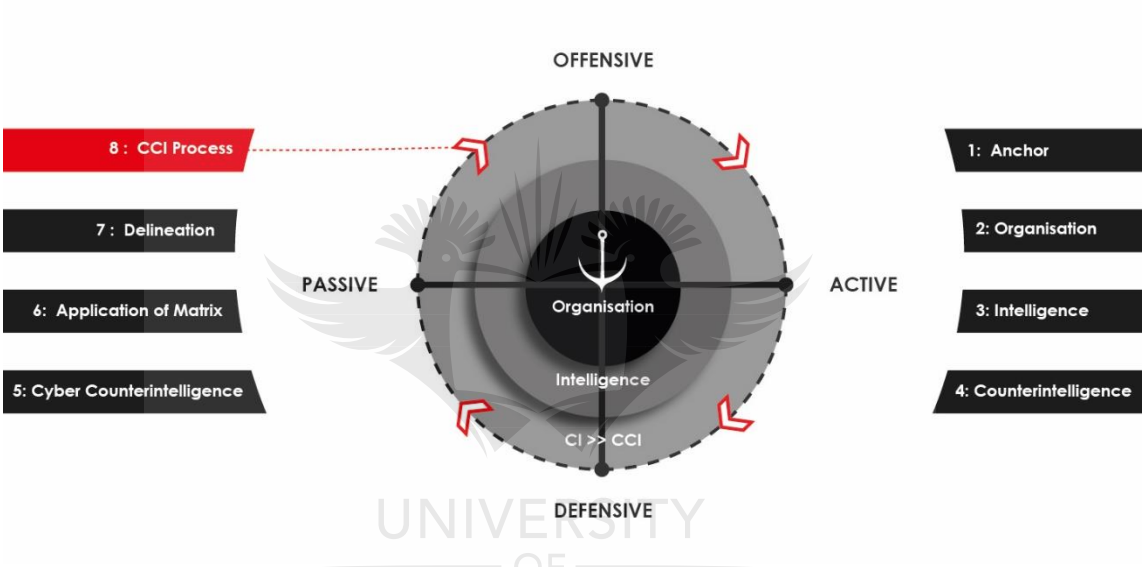


Figure 34: Building Block 8 – CCI Process (Duvenage, Sithole & von Solms, 2017)

It is practically and academically infeasible to attempt to describe the CCI process in all its detail. The notional structuring of CCI calls for a simplification at a higher level of abstraction. At this higher level, a bird's eye view emerges of the process that coherently binds and drives the work of CCI. A process model is a construct that can offer this bird's eye view.

As **process models** in general, the CCI process model should be presented as a construct acting as “idealizations of processes that are more subtle and more complex in practice” (Berkowitz & Goodman 2000). A model ought to be simultaneously congruent **with** reality and an idealised, simplified representation **of** reality. It parsimoniously explains a process that encompasses diverse activities and elements. Since it is an idealisation, a model is “an aim point, of what the process should look like

if everything goes as planned" (Lowenthal 2012). Academically, a process model serves as a notional concept for theorising and a premise or soundboard for research. More practically, a model provides a template for the organised execution of functions and activities.

A process model typically consists of graphically depicted and narratively explained step-by-step actions. An academically credible CCI process model cannot be presented as 'standalone'. It should consider some existing postulations on not only the CCI process, but also other process models in related fields. This broader approach is reflected in our structuring of the rest of the chapter, namely:

- Section 13.2: CCI process model – Why it is Needed and Important as a building block
- Section 13.3: Overview of some existing process models
  - Subsection 13.3.1: Existing propositions on the cyber counterintelligence process
  - Subsection 13.3.2: Propositions on the cyber intelligence *a*nd cyber threat intelligence processes.
  - Subsection 13.3.3: Are there other alternatives in Intelligence Studies and Business Intelligence useful to constructing a CCI process model?
- Section 13.4: Proposal for a CCI process model
- Section 13.5: The CCI process model and institutional maturity
- Section 13.6: Conclusion

In explaining the above, this chapter draws on, and contains verbal extracts from Duvenage, von Solms & Corregedor 2015, Duvenage & Hough 2011 as well as Duvenage 2011.

In this section, we introduced the CCI process as a building block and explained the approach followed in the chapter with regard to its construction. We now proceed with discussing the need for, and importance of, the building block.

13.2 CYBER COUNTERINTELLIGENCE PROCESS MODEL – WHY IT IS NEEDED AND IMPORTANT AS A BUILDING BLOCK

Properly contextualised, the foregoing seven building blocks (Chapter 5–12) provide all the 'parts' necessary to academically explain and practically execute CCI. At this juncture, these parts – and thus the FCCI – are still 'static'. They lack the dynamism that synergistically combines and drives these different parts as an integrated process

(Duvenage, von Solms & Corregedor 2015). Consequently, a description of the CCI process is needed as the FCCI's last building block. For reasons noted in Section 13.1 this is best done by considering some existing process propositions and then designing a CCI process model most suited to our FCCI.

Extending from Section 13.1, we can infer two further reasons for the importance of a CCI process model. Firstly, on an academic level, a process model serves as a notional concept for directing and delineating further research on CCI. Secondly, on a practical level, the conceptual outline of the process provides an organising template for performing CCI work in practice. On both counts, the CCI process model is (to paraphrase an earlier assertion in Section 13.1) an idealisation and aim point of what the CCI process should look like to be optimally effective when everything goes as planned.

We now proceed with reviewing some existing propositions on the CCI and related processes.

13.3 OVERVIEW OF SOME EXISTING PROCESS MODELS

From the outset, the CCI process needs to be distinguished from the cybersecurity process. Over the years, the term ‘cybersecurity’ process has come to denote the cluster of compliance-driven activities in which the technical aspects predominate. The implementation and adoption practices prescribed by ISO 27001 and ISO 22301 were, and are still, seen as providing cybersecurity processes for all types of entities (Duvenage, von Solms & Corregedor 2015). While critically important, such processes are wholly insufficient on their own in safeguarding and advancing organisational interests.

13.3.1 EXISTING PROPOSITIONS ON THE CYBER COUNTERINTELLIGENCE PROCESS

In as far as the consulted academic and published literature is concerned, contributions on models that pertinently deal with the CCI process are rare. For example, one of the most authoritative works on CCI, Bodmer *et al.*’s (2012) *Reverse deception – Organized cyber threat counter-exploitation* does not advance such a process. Two notable academic works that do address the CCI process are Sigholm and Bang’s paper (2013) 'Towards offensive cyber counterintelligence' and Fieber’s (2015) master's capstone *The Iranian computer network operations threat to U.S. critical infrastructures*. In the two subsections that follow we appraise these two contributions.

13.3.1.1 Offensive CCI Attribution Process

With the qualification that their paper is placed within a statutory military context, Sigholm and Bang (2013) set out to offer a "comprehensive process that bridges the gap between the various actors involved in CCI". The work subscribes to Clark's (2004) "Target-centric Intelligence Process" which was specifically advanced for statutory intelligence analysis (i.e. not the whole range of intelligence and CI functions). Graphically, Clark's model – which is foundational to Sigholm and Bang's (2013) proposition – can be depicted as follows:

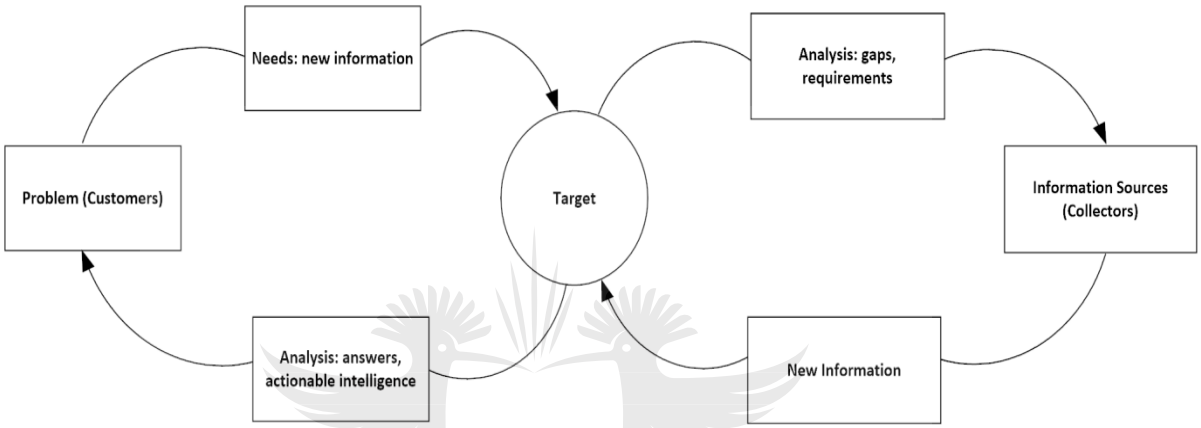


Figure 35: Target-centric Intelligence Process (Clark 2004)

Drawing on Clark's (2004) model, Sigholm and Bang (2013) postulate a model for the "offensive CCI attribution process". Rather than an overarching "comprehensive" CCI process, their proposition is on closer examination limited to one aspect of the CCI process (namely attribution) and more specifically an information flow and analysis architecture to be employed for this (attribution) purpose. In their proposal, offensive CCI is neither incorporated into defensive CCI nor is it dovetailed with the broader CI process. This is illustrated by the following diagram they provide (Sigholm & Bang 2013):

Please see next page for Figure 36.

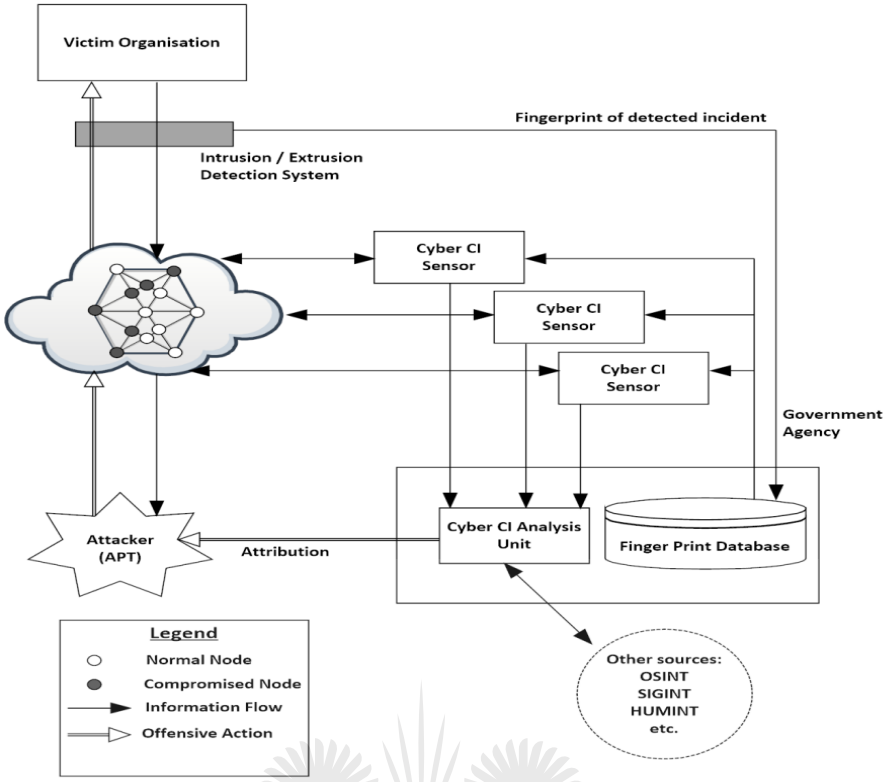


Figure 36: Layout of the Offensive CCI Attribution Process (Sigholm & Bang 2013)

Subsequent to Sigholm and Bang's (2013) proposition, an outstanding and more comprehensive CCI process model was advanced by Fieber (2015). This model is discussed in the next subsection.

13.3.1.2 *Organisational CI model in cyberspace*

Fieber (2015) rests his proposition on two key contentions which also underpin our proposal on a CCI process model (See Section 13.4). Firstly, asserts Fieber (2015), the CCI process spans across “domains” in the sense that it “incorporates both technical and non-technical countermeasures”. Secondly, CCI “mirrors the conventional CI process and the two cannot be separated” (Fieber 2015). Fieber (2015) proceeds with postulating the “general phases” of the CI/CCI process as (1) assess; (2) identify; (3) exploit; and (4) neutralise. Fieber (2015) then overlaps the CI process's phases with the stages of the “active cyber defense cycle”. The stages of the "active cyber defense cycle", as described by Fieber (2015) are: (1) asset identification and network security monitoring; (2) incident response; (3) threat and environment manipulation; and (4) threat intelligence consumption. Fieber (2015) graphically depicts the resultant “organizational CI process model” as follows:

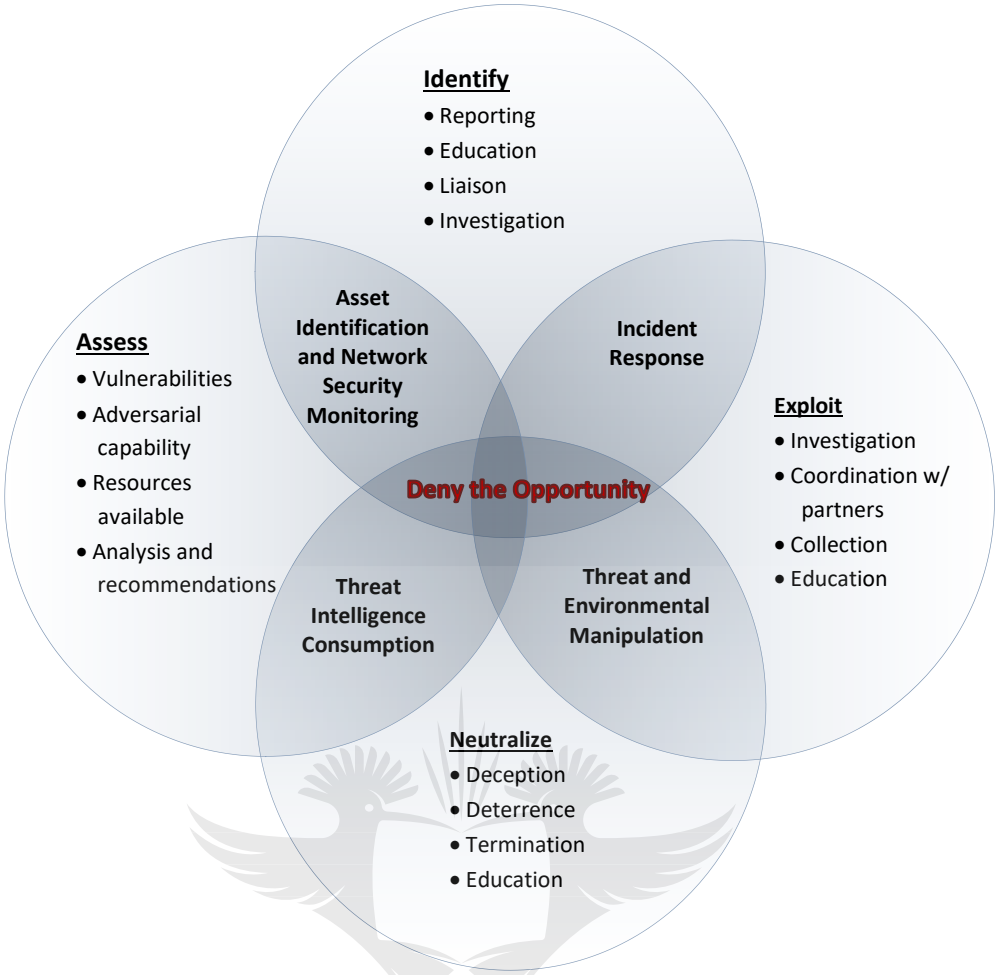


Figure 37: Organizational counterintelligence model to deny adversaries the opportunity to achieve effects in cyberspace (Fieber 2015)

Fieber (2015) continues with substantiating his model with reference to the countering of Iranian “cross-domain threats”.

Parallel and independent research at the University of Johannesburg also aimed at designing a CCI process model (Duvenage, von Solms, & Corregedor 2015). Predating Fieber’s (2015) capstone project’s publication (in August) by two months, the outcome of the University of Johannesburg's research was published in June 2015 as part of the *Proceedings of the 14th European Conference on Cyber Warfare and Security* (Duvenage, von Solms, & Corregedor 2015). In their paper titled, 'The cyber counterintelligence process – A conceptual overview and theoretical proposition’, Duvenage, von Solms and Corregedor (2015) propose a CCI process that is more granulated than Fieber's (2015). Duvenage, von Solms and Corregedor's (2015) model, which is presented in Section 13.4 of this chapter, is based on an appraisal of existing processes models not only within CCI, but also pertinent proposals in the related fields of 'cyber intelligence, 'cyber threat intelligence', Business Intelligence and Intelligence

Studies. Since an appraisal of propositions in related fields is congruent with the academic rigour required of a doctoral l thesis, the next two subsections comprise:

- Subsection 13.3.2: Positions on the 'cyber intelligence' and 'cyber threat intelligence' processes
- Subsection 13.3.3: Alternatives in Intelligence Studies and Business Intelligence

13.3.2 PROPOSITIONS ON THE CYBER INTELLIGENCE AND CYBER THREAT INTELLIGENCE PROCESSES

The literature published by cybersecurity entities offering CCI services do in some instances contain references to the CCI process. These vendors' contributions are cursory, aimed at expanding market share, and not substantiated academic research. None of the promotional publications reviewed purport to offer a model specifically linked to the CCI process (Duvenage, von Solms & Corregedor 2015). However, as noted earlier, 'cyber intelligence' and 'cyber threat intelligence' should be examined for insights useful to the design of our CCI process model. Consequently, we now proceed with propositions with these tags.

Process propositions under the tags 'cyber intelligence' and 'cyber threat intelligence' are certainly not in short supply. Various of these propositions strongly draw in their descriptions of the 'cyber intelligence' process on what is known in Intelligence Studies as the traditional intelligence cycle (Duvenage, von Solms & Corregedor 2015). As it has done for more than 60 years within Intelligence Studies and statutory intelligence practice (Hulnick 2007), the traditional intelligence cycle now strongly influences thinking on processes in the cyber realm. Reduced to its essence, the intelligence cycle comprises the activities of direction, collection, analysis and dissemination. Graphically Figure 38 depicts the intelligence cycle as follows:

Please see next page for Figure 38.

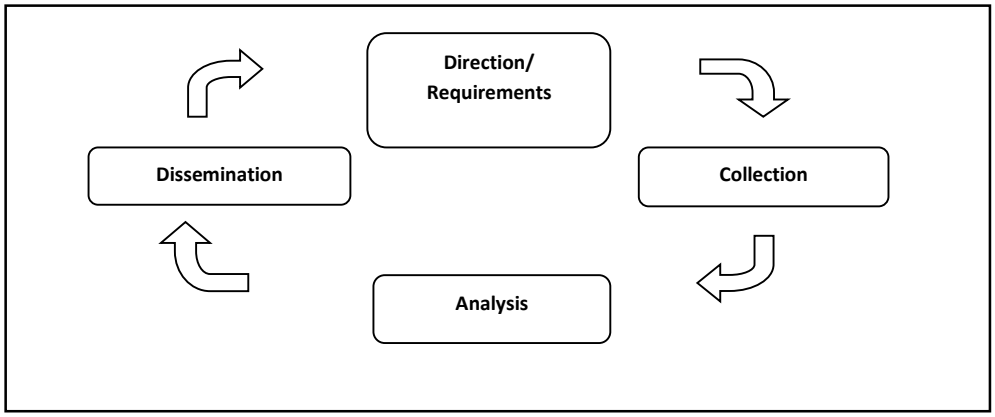


Figure 38: Traditional Intelligence Cycle (Author)

Within the cybersecurity sphere, subscription to the intelligence cycle varies from simple adoptions at one end of the spectrum to customised expansions at the other end of the spectrum. Serving as an example of a simple adoption is VeriSign's (2012) *Establishing formal cyber intelligence capability (White Paper)* which states: "To successfully mount and implement an intelligence capability, it's essential to understand the intelligence lifecycle model … [the]…Traditional Intelligence Cycle comprise of Direction, Collection, Analysis and Dissemination." This description concurs exactly with the cycle depicted in Figure 38.

At the other end of the spectrum, KPMG (2013) advances the following customised, expanded proposition as a **basic intelligence operating model** for "cyber threat intelligence" – graphically depicted as follows:

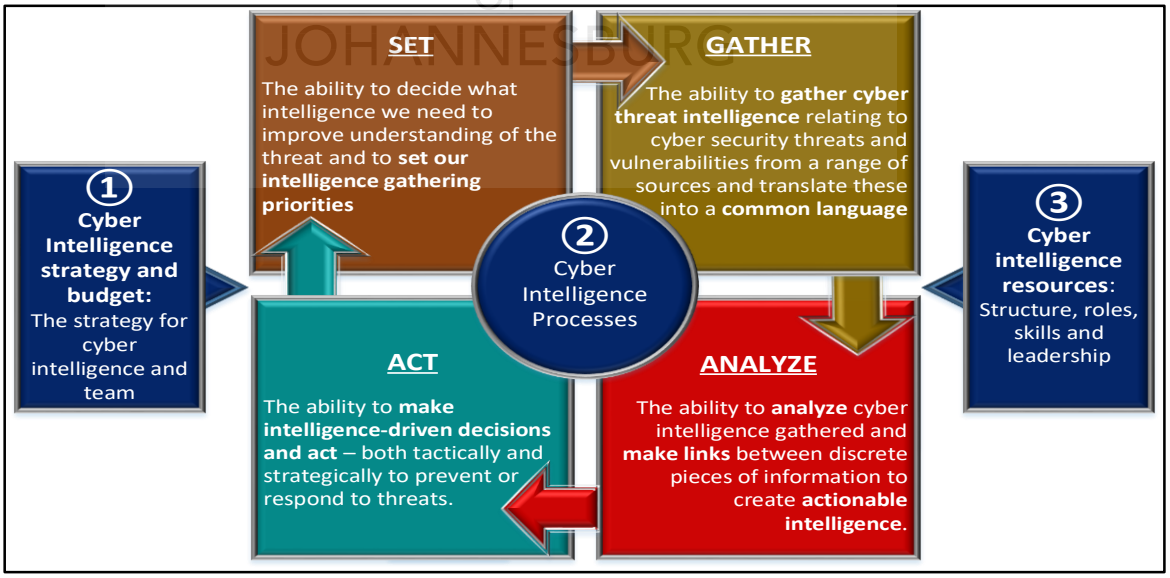


Figure 39: Basic Intelligence Operating Model (KPMG 2013)

As would have been noted, the intelligence cycle in its simple or expanded format does not explain or even mention CI or CCI. As is the case in Intelligence Studies, proponents of this cycle in the cybersecurity realm may argue or imply that CI (and by implication CCI) is performed throughout the cycle (c*f*. Lee 2014a–e, VeriSign 2012). The CI process, proponents argue, mirrors and protects the intelligence cycle (Duvenage & Hough 2011). In reality, these counterintelligence-throughout-the-cycle and counterintelligence-follows-the-cycle positions simply do not work. The intelligence cycle was originally conceived to explain positive intelligence, but is not particularly good at that either (Duvenage & Hough 2011). The following observation by Arthur Hulnick (2007), a distinguished intelligence practitioner and Intelligence Studies scholar, is just as applicable to the cyber field:

> …[t]he intelligence cycle is a flawed vision, and thus poor theory. One need only ask those who have toiled in the fields of intelligence...[C]ounterintelligence follows an entire different and unique path of its own...It has nothing to do with the intelligence cycle. Instead there is counterintelligence methodology that is unique...So when one looks at the pattern of counterintelligence functions, it does not look at all like the intelligence cycle.

If the intelligence cycle does not work for CI generally, it can of course not work in the cyber realm generally and for CCI specifically.

In this section, we overviewed propositions on the CI and cyber threat intelligence process models for possible use in designing our CCI process model. We found various such models to be based on the flawed, traditional intelligence cycle orientating from Intelligence Studies. We conclude that such models do not accurately depict the CI process and can thus not be applied to the CCI process. In the next section, we examine the question whether there are other alternatives that can inform our design of the CCI process model.

13.3.3 ARE THERE ALTERNATIVES IN INTELLIGENCE STUDIES AND BUSINESS INTELLIGENCE THAT ARE USEFUL FOR CONSTRUCTING A CYBER COUNTERINTELLIGENCE PROCESS MODEL?

Contrary to what might have been expected, no current postulations offer a quick-fix solution. Endeavours within Intelligence Studies over the past two decades to offer alternatives remain overwhelmingly directed at positive intelligence (*cf.* Johnson 2007, Lowenthal 2012, Clark 2004). One of the few propositions pertinently advanced for CI is that by Hulnick (2007). He proposes a “counterintelligence model” comprising a five-

clustered “pattern”, namely “identification”, “penetration”, “exploitation”, “interdiction” and “claim success”. Summarised, Hulnick’s (2007) description of the phases of the CI model is as follows:

- Identification of espionage adversaries
- Penetration of adversarial espionage intelligence structures
- Exploitation, which refers to the collection of information (on adversaries) and the institution of measures such as deception
- Interdiction, which ensues when the “the case is turned over to law enforcement”
- Public declarations by state authorities of successful counterintelligence actions

Hulnick (2007) explicitly limits the model above to “active counterintelligence”, but adds the qualification that “defensive measures in counterintelligence” do not fit into “either the traditional intelligence cycle or the model [he] just described.” Within state security structures, these long-established defensive measures are commonly referred to as operational security (OPSEC) and comprise the following five steps (US 1996):

(1) Identify critical information and other assets.
(2) Analyse threats.
(3) Determine vulnerabilities.
(4) Assess risks.
(5) Develop and implement countermeasures.

Effective CI and thus CCI require the integrated execution of offensive/active and defensive/passive modes. They are, after all, different sides of the same coin. Are there examples of integrative proposals which combine defensive and offensive CI dimensions? While none could be found in conventional Intelligence Studies, propositions exist within Business Intelligence which attempt to combine the offensive and defensive missions. A seminal model in this regard was forwarded by Nolan (1997). While copyright restriction prevents inclusion of Nolan’s graphical depiction in this paper, subsequent Business Intelligence propositions convey the same thinking. The following proposal by Brouard (2004) shown in the following figure is an example:

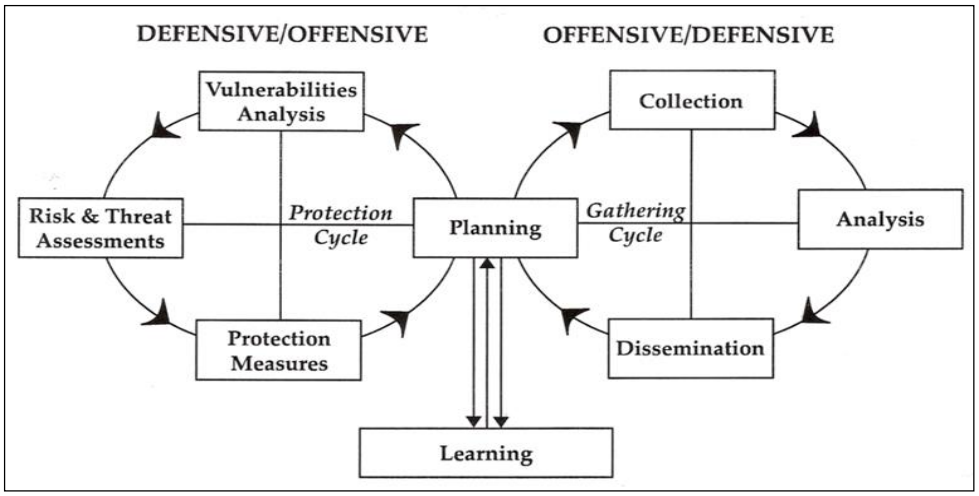


Figure 40: Intelligence Gathering and Protection Intelligence Process (Brouard 2004)

Such models are a useful contribution in their conceptual integration of subprocesses and the additional risk assessment methodology. Nonetheless, they insufficiently reflect the nature of the defensive and offensive CI mission. They are also not granulated enough to serve either as an aiming point for practical execution or as a sounding board for further academic exploration.

Drawing on our examination of some existing process models, we now proceed to advancing our own CCI process model.

13.4 PROPOSAL FOR A CYBER COUNTERINTELLIGENCE PROCESS MODEL

We propose a model that combines the respective steps of offensive and defensive CI (and thus CCI) in a single process. Within this process, the defensive and offensive subprocesses (while for the large part intertwined) also follow a distinctive pattern of steps. The detailed description of both the subprocesses is an extensive task – especially within the confines of a thesis already advancing several other notional constructs. Therefore, this section narratively describes only the offensive subprocess.

CCI, to re-emphasise, is executed as part of the broader CI process. The CCI process thus looks, works with and is inseparable from the CI process. Graphically, the CCI process can be depicted as follows:

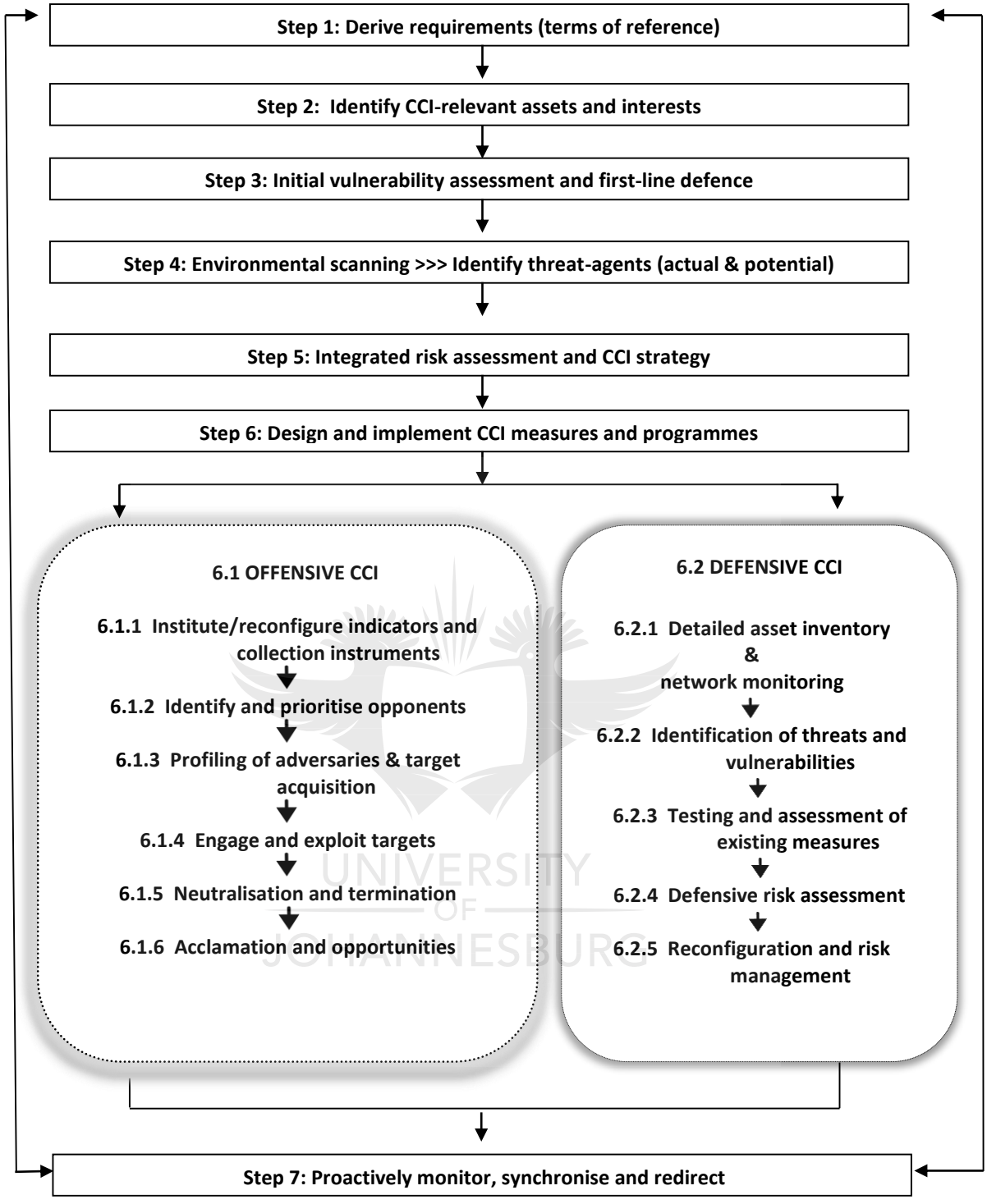


Figure 41: Cyber Counterintelligence Process Model (Adapted from Duvenage, von Solms & Corregedor 2015 and Duvenage & Hough 2011)

Although Figure 41 shows a linear sequence (i.e. neat finalisation of one step, directly followed by the execution of the subsequent steps), the CCI process is in reality multidirectional with steps being repeated and crisscrossing. This qualification also applies to the narrative description of the model in the paragraphs that follow.

Step 1: Derive requirements (terms of reference)

Like CI in general, CCI is not an end in itself. It serves the interest of a particular client, be it a government or a business. The client expects its CI apparatus to not only safeguard its vital interests and objectives, but also to actively advance these. Ideally, CCI (as part of the broader CI process) would commence with the client clearly expressing its expectations. These would include what cyber assets should be protected and what CCI should do to proactively promote government or company interests. While the soliciting of CCI services from a specialised company might come with a neatly packaged 'wishlist' with clear-cut, all-encompassing requirements and priorities, this is very rarely the case. CI and CCI requirements are mostly derived and not received. They are derived through a meticulous appraisal of the client's objectives, intentions and strategy. Preferably these should be contained in terms of reference (ToR) endorsed by the client and in stating the obvious within the parameters of legal jurisdictions.

Step 2: Identify assets to be protected and interests to be advanced

Resources are finite and CCI can only execute its signature role to defend and neutralise in a highly prioritised and selective manner. Ascertaining what assets and interests in the information cybersphere are worthy to protect and advance by expending precious resources is the right place to start. In the case of nation states (or other sizable role-players), these information cyber assets and interests (identified on the basis of the ToR) are threefold:

(1) Assets the state possesses which are central to survival and prosperity (such as critical bodies of information, systems and infrastructure)
(2) Assets the state aspires to procure by cyber means (such as the secrets of adversaries)
(3) Interests refer to the conditions the state seeks to realise (e.g. gaining a competitive edge over an adversary by obtaining such secrets, adding additional layers to its defences or offensively undermining the C-I-A of adversarial systems)

Step 3: Initial vulnerability assessment and firstline defence

Although there are exceptions, CI doctrine requires offensive action to be preceded by solid defence. Applied to CCI, the identification of real and aspirational assets and interests described above is therefore followed by ascertaining vulnerabilities in defensive, cybersecurity measures which protect these assets and interest. This compliance driven-process would typically result in remedial action in relation to cyber-, information, physical and personal security. It thus also involves CI specialisation fields

other than CCI. This subprocess is again performed, but more exhaustively, as part of Step 6.2. However, care should be taken not to summarily close all the 'holes' in the cyber 'fences'. Some of these could be exploited for offensive purposes (such as deception) later on in Step 6).

Step 4: Environmental scanning – Identify threat agents (actual and potential)

In the assessment just performed, we mostly considered internal weaknesses and vulnerabilities. Effective CI has to safeguard against and also engage external threats. While opponents (competitors and adversaries) are common threat actors, risks can also be posed by technological and socio-political developments. While all of these are not of concern to CI and CCI, they are considered inferring actual and potential threat-agents (of CI relevance). A common pitfall is to identify threat agents mainly on the basis of actors known to be active, adversarial and well capacitated. The result is a self-feeding, atrophic CCI process with risks posed by threat actors going undetected. The importance of innovative environmental scanning, directed by the ToR, and aimed at identifying potential threat agents can thus hardly be overemphasised.

Step 5: Integrated risk assessment and strategy

Considering the external and internal threats as well as vulnerabilities and weaknesses identified in the preceding steps, the CCI process proceeds to an integrated risk assessment. The risk assessment pronounces on what CCI measures are obsolete, which require modification and in which areas they are lacking. Decisions on CCI are formulated as part of a broader CI strategy which combines defensive and offensive dimensions. As suggested earlier, a balance has to be maintained between (to paraphrase Nolan 1997) the defensive CI task to 'close holes in the fence', and offensive CI that seeks to exploit the offensive opportunities that vulnerabilities offer.

Step 6: Design and implement CCI measures and programmes

While offensive and defensive CCI are designed and implemented in synergy, the subprocess each has a unique mission and thus pattern of execution. This chapter, as noted earlier, is limited to narratively describing the **offensive** pattern (**Step 6.1, Figure 41**) which consists of the following six substeps:

(1) *Substep 6.1.1: Institute/reconfigure indicators and collection instruments.* Since espionage is both a precursor and end goal of sophisticated cyber breaches, the offensive subprocess commences with instituting and/or reconfiguring (a) indicators of adversarial cyberespionage and (b) own collection instruments. Whatever form these instruments take (honeynets, tarpits, footholds in relevant

online communities and sites, etc.), they will be developed and are constantly fine tuned around those assets most prized by opponents. In Steps 6.1.3 and 6.1.4, these instruments will be accustomed even further to best collect on and then engage targets.

(2) *Substep 6.1.2: Identify and prioritise intelligence opponents.* In addition to information obtained through the preceding step, CCI will draw on the broader, all-source CI picture to identify those opponents actually and potentially to be targeting the own entity though intelligence actions such of espionage, covert action, and so on. Even the well-resourced entities cannot offensively focus on all known and suspected opponents. Consequently, only prioritized opponents are elevated to actual/potential adversaries and pursued through further offensive action.

(3) *Substep 6.1.3: In-depth 'profiling' of adversaries to arrive at targets.* These offensive actions firstly entail the focused collection of information on and subsequent in-depth profiling of adversaries. The focused collection of information involves high-risk and high-cost measures and could include cyberespionage. One of the crucial CCI collection requirements is to ascertain the instrumentalities and proxies an adversary uses for intelligence activities. To this end, information procured through other conduits such as HUMINT and other TECHINT are also used. Depending on various factors, some of these adversaries, their proxies or campaigns not suited to offensive exploitation will be handed over to be dealt with by defensive CCI.

(4) *Substep 6.1.4: Engagement and exploitation of targets.* As is clear from the above, the acquisition of targets (prioritised adversaries and their proxies) for offensive action is an exhaustive process. In certain respects, the acquisition of targets is the most complex part of CCI work. To adopt a target-centric-type view like that of Clarke (2004) at the start of the process would thus clearly be a gross oversimplification that skips critical segments of CCI methodology. The engagement and exploitation of targets are at the core of offensive CCI. This exploitation can take myriad forms and include escalated (more aggressive) collection, deception, manipulation, disinformation and disruption of hostile intelligence activities. The ideal aim of CCI is to degrade and control the adversary through his own cyberaction. The following observation by Codevilla (1992) rings true also in respect of CCI: "Action against the enemy through the enemy's own intelligence is the very consummation of CI." Usually this is best achieved by combining CCI with other forms of offensive CI. Deception through honeynets could, for example, be supplemented by means of disinformation fed

to an adversary through a human double agent. Although not strictly part of civilian CCI, offensive actions could in the military context include pre-emptively lining the digital battle for cyberwar.

(5) *Sub-step 6.1.5: Neutralisation and termination.* While the targets are to a certain level neutralised through exploitation, offensive CCI operations typically have a 'neutralisation and termination' phase at the end of their 'life-cycle'. Such termination can either be opted for (i.e. at own initiative at a predetermined time) or necessitated by circumstances (such as indications that an operation has been compromised). Whatever the case, termination should be planned for in advance and utilising various scenarios. Termination thus planned has two purposes. Firstly, it delivers the final neutralisation ‘blow’ to the adversaries’ campaigns being engaged. Secondly, if executed skilfully, it could provide the 'seeds' for subsequent 'generation' of CCI operations.

(6) *Sub-step 6.1.6: Acclamation, reflection and identification of further opportunities.* As with CI generally, CCI success ought to be followed by acclamation. Acclamations are of two kinds. Firstly, public acclamation involves citing aspects of the successful countering of malicious cyber intelligence activities (such as organised cybercrime). In democratic countries, such claiming of success is vital in justifying in the public eye the billions spent on intelligence, CI and CCI work. Furthermore, public acclamation can be part of degrading an adversary. Secondly, acclamation can be limited on the basis of the need-to-know principle. Sometimes entities “try hard to keep successes secret so that they might be repeated. An oft-quoted CIA saying is, ‘The secret of our success is the secret of our success.’“ (Hulnick 2007). From a management perspective, peer commendation is imperative in ensuring continued devotion to CI, which is an exhaustive task conducted in secret over a long period of time. Whatever acclamation opted for, CCI operations are assessed for lessons learned and to identify opportunities for further exploitation.

Step 7: Monitor, synchronise and redirect

Although indicated as a separate step in the interest of simplicity, CCI is continuously monitored and synchronised and redirected in accordance with the broader CI and intelligence effort. The latter, in turn, ought to be dovetailed with an entity’s objectives and strategy. Intelligence and CI of any kind are instruments, not ends in themselves. The intelligence and insights gained through this endeavour influence objectives and strategy, and thus eventually the ToR of the ongoing intelligence process of which CCI is but a part.

In this section, a high-level proposition on a CCI process model was advanced. As will be observed, our model is considerably more detailed than, but share essential features with, Fieber's (2015) proposition. In the next section observations are made on the relationship between the CCI process model and institutional maturity.

13.5 THE CYBER COUNTERINTELLIGENCE PROCESS MODEL AND INSTITUTIONAL MATURITY

In the context of its use in this thesis and chapter, the term 'process model' refers to the range of activities an institution performs to execute its core business. The optimal execution of the CCI process presupposes advanced levels of institutional maturity in respect of structures, people, technologies, policies and procedures as well as skills development (Jaquire, Duvenage & von Solms 2018). Attaining such CCI institutional maturity is in itself an on-going process that would by its very nature differ, in form and content, from the CCI process model advanced in this chapter. A detailed discussion of CCI maturity will distract from the thesis's focus. This thesis was qualified as advancing a high-level, overarching CCI framework. Furthermore, CCI maturity has been the focus of a dedicated research stream at the University of Johannesburg that recently culminated in the completion of a separate doctoral study (University of Johannesburg 2018; Jaquire 2018; Jaquire & von Solms 2017 a-c). For purposes of our FCCI's design, we thus note the importance of CCI maturity, but do not elaborate further on this aspect.

This section observed on the relation between our FCCI's eight building block (the CCI process) and CCI maturity. We now proceed with concluding the chapter.

13.6 CONCLUSION

In this chapter, we explained the importance of a CCI process model as our FCCI's final building block. We examined some existing process models and, with the exception of Fieber's model (2015), found these to be insufficient for explaining CCI. In the main, these models do not compute CCI's defensive and offensive CCI missions. Moreover, they are not granulated enough to serve as an aimpoint for the practical execution of CCI or a sounding board for directing academic research. Therefore, we proceeded with postulating a CCI process model which gives a bird’s eye view of the overarching process that coherently binds and drives CCI. Employed as an FCCI building block, the CCI process model we designed synergistically combines and adds 'dynamism' to the preceding seven building blocks of our FCCI.

This chapter concludes the construction of our FCCI and thus Part 3 of the thesis. We now proceed to Part 4, which apply the integrated FCCI as an organisational training tool (Chapter 14).

PART 4

THE FCCI AS AN ORGANISATIONAL TRAINING TOOL

Part 4 explores the FFCI's application as a tool for an organisation's CCI training and awareness programme. It consists of **Chapter 14**.

CHAPTER 14

THE FCCI AS AN ORGANISATIONAL TRAINING TOOL

14.1 INTRODUCTION

In Chapters 4-13 we presented the FCCI and its components. Throughout the thesis we emphasised the requirement for our FCCI to not only serve an academic construct, but also to have practical application. Albeit cursory, Chapters 10-13 did illustrate some aspects of our FCCI's practical application through, for example, our proposition on the CCI process and the CCI matrix's illustration by means of a case study. This was done to validate the thesis primary hypothesis that a credible framework can be designed to explain what CCI is and how 'it works'. In explaining the thesis's problem statement (Chapter 1), we furthermore suggested that a key measure of our FCCI academic credibility would be the contribution it makes to structuring CCI as a "topic of instruction". More concretely, this means that to be credible our FCCI (advanced in preceding chapters) should have practical use in CCI training. The aim of this chapter is precisely this – namely to illustrate the FCCI as a conceptual construct practically useful to an organisation's CCI Awareness and Training Programme (ATP). This chapter expands on peer-reviewed research by Sithole, Duvenage, Jaquire and von Solms (2019).

CCI, and even more so CCI training, are niche fields not necessarily familiar to all readers of this thesis. Therefore, for the discussion of our FCCI as part of an ATP to make sense, the chapter first needs to provide some **background** on the broader concept of CCI Awareness, Education and Training (**AET**) and its complexities more generally. This is done per **Section 14.2**.

Moving from this broader base, the chapter then proceeds with **Section 14.3**. In this section we shall more specifically discuss a **CCI Awareness and Training Programme (ATP) as a subset of CCI AET**. As part of this discussion we advance a proposal on a generic organisational CCI ATP which incorporates our **FCCI** as a training tool.

The rest of the chapter is structured as follows:

- Section 14.2: Cyber Counterintelligence Awareness Education and Training (CCI AET): Concept and Complexity

- Subsection 14.2.1: Conceptualising organisational CCI AET
- Subsection 14.2.2: The importance of considering organisational context in designing CCI AET
- Subsection 14.2.3: The role of the FCCI in CCI AET

- Section 14.3: Towards an Organisational Cyber Counterintelligence Awareness and Training Programme (CCI ATP)
  - Subsection 14.2.1: Conceptualising an organisational CCI Awareness and Training Programme (ATP)
  - Subsection 14.2.2: The FCCI as a CCI Awareness and Training Programme (ATP) tool
  - Subsection 14.2.3: The CCI Awareness and Training Programme's (ATP'S) Design and Implementation process
  - Subsection 14.2.4: A cursory overview of a CCI Awareness and Training Programme (ATP)
- Section 14.4: Conclusion

14.2 CYBER CI AWARENESS EDUCATION AND TRAINING (CCI AET): CONCEPT AND COMPLEXITY)

In order to establish a foundation for presenting a CCI ATP (in Section 14.2), this section examines the concept and complexities of CCI Awareness, Education and Training (AET) more generally.

14.2.1 CONCEPTUALISING ORGANISATIONAL CCI AET

CCI's effective implementation and execution above all requires a skilled CCI workforce and CCI-conscious employees. Such awareness and skilling is best achieved as part of a coherent broad-based CCI awareness, education and training (AET) endeavour. As AETs in general, a CCI AET is not a single, uniform "training" program but have three distinct functions, namely 'awareness', 'education' and 'training' (Kissel & Wilson 2010). Each CCI AET function differs in target group, specific objectives, outcomes, content and approaches (Kissel & Wilson 2010).

These functions can be differentiated in more detail as follow:

- **Awareness** is about being cognisant or knowledgeable of a situation or one's surroundings. Awareness constitutes an AET's critical base function - the first line of defence that affords employees with an opportunity to learn about the

importance of personal security as well as protecting an organisation's critical information systems assets. The NIST Special Publication 800-16 defines an awareness as "a learning process that sets the stage for training by changing individual and organisational attitudes to realise the importance of security and the adverse consequences of its failure" (de Zafra *et al* 1998).

- **Education** denotes the facilitation of learning or teaching and the gaining of knowledge. Caballero (2017) describes education as "a formal curriculum created for the purpose of educating individuals in a broad array of security topics that will build a body of knowledge essential for a career in information security". For purpose of this chapter, 'education' is deemed as a function provided by tertiary and training institutions outside the organisation. It is thus not a function provided ***by*** the organisation ***for*** the organisation.
- **Training** pertains to the acquisition of competence (knowledge, skills and attitude) to improve performance and enhance expertise for a specific job or function. Amankwa, Loock and Kritzinger (2014) define training as "any endeavour that is undertaken to ensure that every employee is equipped with the information security skills and information security knowledge specific to their roles and responsibilities by using practical instructional methods such as seminars and workshops".

This subsection explained a CCI AET's three functions. In the subsection to follow we examine the importance of organisational context in shaping the CCI AET endeavour.

14.2.2 THE IMPORTANCE OF CONSIDERING ORGANISATIONAL CONTEXT IN DESIGNING CCI AET

Like the CCI endeavour in general, effective CCI AET is not a standalone 'plug in' or 'add on'. The design of CCI AET should consider the following aspects of organisational context which are unpacked in this section:

- Subsection 14.2.2.1: Organisational objectives, strategy, intelligence and counterintelligence endeavours
- Subsection 14.2.2.2: Organisational type, maturity and the requirements for CCI AET

14.2.2.1 Organisational objectives, strategy, intelligence and counterintelligence endeavours

The design of a sound CCI AET duly considers the wider organisational strategy, intelligence and CCI efforts. This interconnectedness, which underlines the organisational synergy we have expounded in Chapter 6, shapes the CCI AET's design

and consequently the use of our FCCI as part CCI AET. For purposes of this chapter, the said synergy can be depicted as follows:

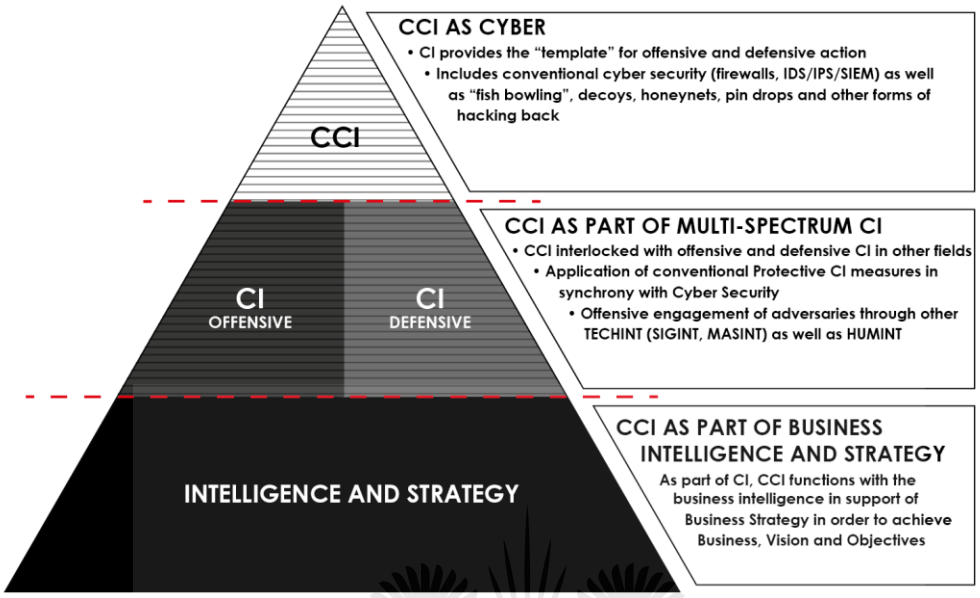


Figure 42: Organisational Strategy, CI and Cyber (adapted from Duvenage & von Solms 2013, Sithole et al 2019) [15]

Implicit to Figure 42 above, is the notion that CCI AET should extend beyond conventional cyber security awareness and training. Instead, CCI AET is a combination of traditional CI and cyber security as well as advanced technical abilities (Black 2014, Van Derwerken & Ubell 2011). In keeping with the thesis's key contentions, Figure 42 shows CCI as being proactive and including offensive dimensions. It therefore encompasses, but is wider than typical cyber risk management and conventional, specialised cyber security measures. Furthermore, CCI requires a sound understanding of the organisational intelligence and counterintelligence endeavours. CCI thus cuts across multiple disciplines and involves several skillsets (Black 2014, Van Derwerken & Ubell 2011). CCI AET draws an all these disciplines and skillsets – with self-evident implications for the complexity of its design.

In this subsection, we examined the importance to a CCI AET's design of organisational objectives, strategy, intelligence and CI. In the next subsection we explore the impact of organisational type and maturity on CCI AET.

[15] As will be observed, Figure 42 is a redesign of Figure 17 featured in Chapter 6.

14.2.2.2 Nature of the organisation and its CCI maturity

Organisations differ vastly not only in their missions (‘main business’), but also in size, resources and their workforces’ CCI-relevant skilling and awareness. Therefore, there is no 'one-size-fits-all' CCI AET. Instead, a CCI ATP's design should be congruent with the organisation's unique features.

A CCI AET, as suggested above, considers its workforce’s existing CCI expertise and the target group, that is, asks does the organisation have an assigned CCI team? If not, does the organisation need to train the existing CI personnel in cyber or the existing cyber workforce in CI, or should new personnel be recruited specifically for the CCI function? Of course not all organisations can afford a highly skilled specialised CCI team. In fact, the majority of medium and smaller organisations will not have such a dedicated team. This does not exclude CCI from the organisational cybersecurity approach. On the contrary, it reinforces such a need. In this regard, Jaquire, Duvenage and von Solms (2018) state:” CCI is not necessarily a separate structure. It is rather a manner for existing and some new functionalities within the organisation to work together in a multi-disciplinary approach to achieve the CCI strategic vision and desired outcomes.”

Moreover, employees in general remain the weakest link in the organisational armour and continue to be the main reason of data breaches resulting from cyber incidents (Thomason 2013, Monk *et al.* 2010, Dtex 2017). Since it is important that every employee knows and understands their roles and responsibilities, a CCI AET has to, at the very least, provide for CCI awareness to all employees regardless of occupational group. The various levels of CCI proficiency are further discussed per Subsection 14.3.1.

14.2.3 THE ROLE OF THE FCCI IN CCI AET

In the preceding two sections we explained the complexity of CCI AET and the challenges posed by the organisational context. These challenges include the wide diversity of topics to be considered for inclusion in CCI AET. Ostensibly the complexity and diversity of CCI AET poses a mammoth task. However, reduced to its essence and regardless of the organisational context, **the aim of CCI AET remains the transfer of awareness, skills and knowledge of ‘what CCI is and how it works’**. In preceding chapters, we advanced our **FCCI** and contended that this framework (consisting of eight building blocks) indeed **explains ‘what CCI is and how it works’**. Consequently, the FCCI and its eight building blocks can be utilised as modular components to design

CCI AET. To substantiate the assertion of the **FCCI**'s usefulness to CCI AET, the next section incorporates the FCCI as part of an organisational CCI awareness and training programme (CCI ATP).

14.3 TOWARDS AND ORGANISATIONAL CCI AWARENESS AND TRAINING PROGRAMME (ATP)

The preceding section provided a cursory overview of CCI AET and its complexity. Progressing from this general overview, this section advances the outlines of a CCI awareness and training programme (APT) with specific reference to the utilisation of the **FCCI**. This section is structured as follows:

- Subsection 14.3.1: Conceptualising an organisational CCI Awareness and Training Programme (ATP)
- Subsection 14.3.2: The FCCI as a CCI ATP tool
- Subsection 14.3.3: The CCI ATP's design and implementation process
- Subsection 14.3.4: A cursory overview of a CCI ATP

14.3.1 CONCEPTUALISING AN ORGANISATIONAL CCI AWARENESS AND TRAINING PROGRAMME (ATP)

As noted in the chapter's introduction (Section 14.1), an organisational CCI awareness and training programme (ATP) is located within the broader notion of CCI AET. Phrased differently, an **organisational CCI APT is a subset of CCI AET**. A CCI ATP specifically **excludes 'education'**, since the latter is deemed as a function provided by tertiary and training institutions outside the organisation. As denoted by its composite terms, the CCI ATP thus **consists of 'awareness' and 'training'**. The 'training' function is sub-dividable to three further proficiency levels namely: fundamental, functional and advanced. These resultant four proficiency levels (tiers) of our CCI ATP can graphically be depicted as follow (on the next page):

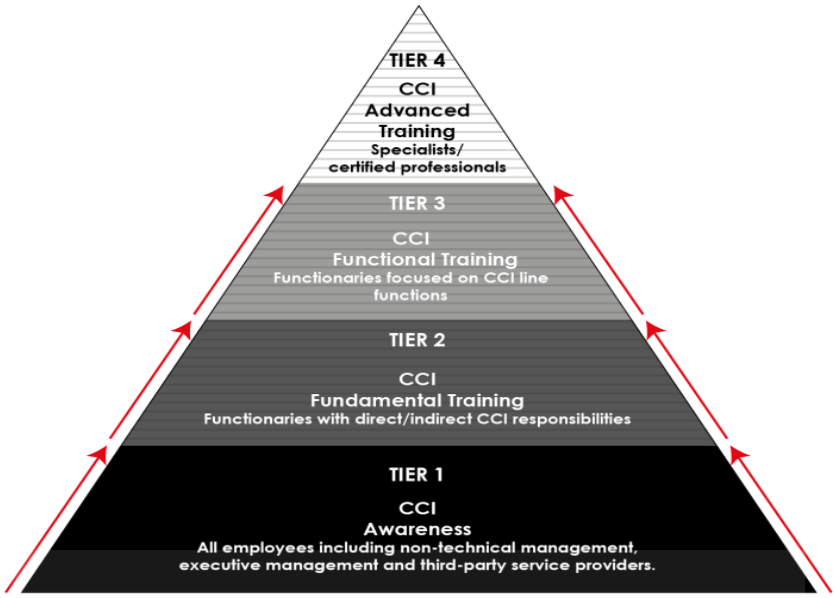


Figure 43: The structuring of Cyber Counterintelligence Awareness and Training (Sithole et al. 2019)

This subsection advanced a high-level conceptualisation of a four-tiered CCI ATP. In the subsection to follow, we examine the use of the FCCI as a tool within a CCI ATP.

14.3.2 THE FCCI AS CCI AWARENESS AND TRAINING PROGRAMME (ATP) TOOL

It will be observed that the CCI ATP per Figure 43 assumes different content and target groups. A further notion underpinning the figure is that the content and/or the depth/detail to which this is covered will vary from target group to target group. The red arrows in Figure 43 depicts this progression in depth and detail from very elementary (Tier 1) to highly advanced (Tier 4).

As with CCI AET of which it is a subset, the CCI ATP's content selection and the level at which it is pitched, will differ according to nature and needs of a particular organisation. Such selection and the development of a CCI ATP is an intricate and challenging process. It is also a process which can conceptually benefit from the application of our **FCCI** as a tool for the selection of **CONTENT** and **PITCH** (i.e. from 'very elementary' to 'highly advanced'). The application of our FCCI as such a training tool can graphically be outlined as follows:

Table 8: Outlining the application of the FCCI as a training tool (Author)

			LEVEL OF AWARENESS AND TRAINING = 'PITCH'									
#		MODULAR CONTENT	Very elementary		→					Highly Advanced/Detailed		
			1	2	3	4	5	6	7	8	9	10
FCCI BUILDING BLOCKS	1	Theory										
	2	Organisation										
	3	Intelligence										
	4	Counter-intelligence										
	5	Cyber CI										
	6	CCI Matrix										
	7	Delineation										
	8	CCI Process										

This subsection explored the application of the FCCI as a tool to conceptually calibrate a CCI ATP. This application is more practically illustrated in Subsection 14.3.4. Prior to the said illustration, we first proceed with positioning the FCCI as part of the CCI ATP design and implementation process.

14.3.3 THE CCI AWARENESS AND TRAINING PROGRAMME (ATP) DESIGN AND IMPLEMENTATION PROCESS

The design and implementation of a CCI ATP, of which our **FCCI** forms part, can graphically be depicted as follows (on the next page):

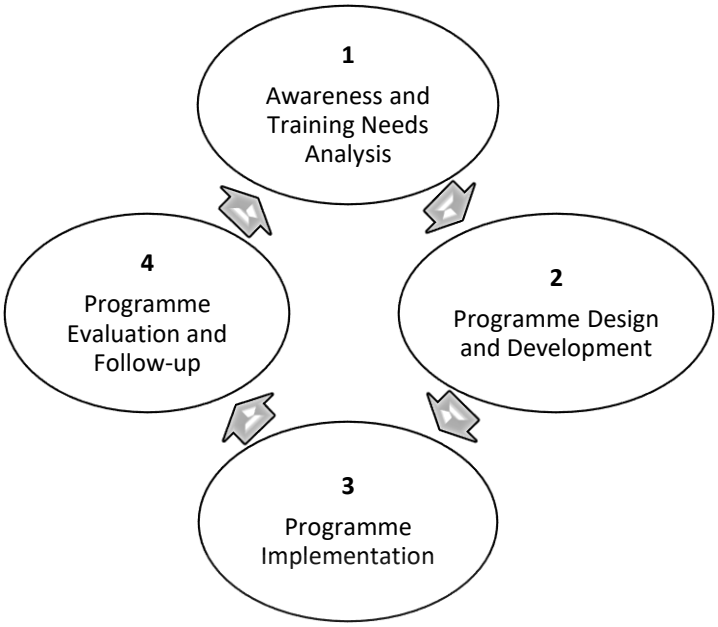


Figure 44: The CCI ATP design and implementation Process (Sithole et al 2019, adapted from MacCauvlei Learning Academy, 2016)

The four critical steps, depicted in Figure 44 comprise the following (adapted from MacCauvlei Learning Academy, 2016):

1) An **awareness and training needs analysis** determines the organisation's awareness and training needs according to the strategic objectives. It looks at the skills and knowledge required by the workforce generally and the CCI team specifically, with due cognisance of the organisation's strategy well as its objectives
2) . The **programme design and development** derives the programme objectives from the training needs and then designs and develops the training material. It determines content, the duration of the programme, the training methods and techniques. The three proficiencies of CCI training (fundamental, functional and advanced – see Figure 43) will be designed according to the functional specialisations such as CCI collection, CCI analysis, CCI investigation, CCI offensive and CCI defensive. To this end the design phase will apply the **FCCI** as a tool to determine content and pitch (See Figure 44 above).

3) The **programme implementation**, communicates the training implementation to the respective target groups and their management echelons. Various training methods can be used for the implementation of awareness and training, such as classroom, online, practical, simulations, on-the-job training and so on.

4) **Programme evaluation and follow-up** appraises the effectiveness of the programme in terms of the increase in knowledge and skills and the improvement of attitude on the job as a result of the awareness and training programme. Follow-ups are done in the workplace after a certain period about the sustainability of knowledge, skills and attitude.

In this section, we advanced a structured process which can be applied for the design and implementation of a CCI ATP. In the next section, we provide a cursory overview of the CCI ATP design and development process's outcome.

14.3.4 A CURSORY OVERVIEW OF A CCI AWARENESS AND TRAINING PROGRAMME (ATP)

The CCI ATP's design *per* the processes described above will a detailed curriculum. For self-evident reasons, such a curriculum cannot not be discussed at length in this thesis. Therefore, we suffice with a cursory overview of the CCI ATP and a high-level application of the FCCI as tool. The overview and application are **categorically qualified** as very **selectively illustrative** and do not in any way purport to reflect all dimensions and content of a CCI ATP.

14.3.4.1 CCI Awareness – the first line of defence and offence (See Tier 1 – Figure 43: The structuring of Cyber Counterintelligence Awareness and Training)

A CCI awareness programme is a first line of defence and a foundation for the stronger cyber security posture of an organisation. Since employees cannot protect information systems against something they are oblivious of, CCI awareness is foundational to enlightening employees of the cyber threats faced individually and as an organisation. It affords employees with an opportunity to learn about the importance of personal security as well as protecting the organisation's critical information systems assets. CCI awareness conveys the possible cyber risks and threats faced by the organisation and provides skills to mitigate basic cyber-related risks and counter cyber threats (Roper, Grau & Fischer 2006). Simultaneously, and even at this very basic level , employees are sensitise that suspected and actual **incidents do not only pose risks, but may also present the organisation with exploitable opportunities**. This mind set should be reflected in incident identification , - handling and -reporting procedures

The key elements of CCI awareness are as follow:

1) Description: A blended cyber security and CI awareness programme that increases employee awareness on the cyber threat landscape, type of adversaries and their techniques, and provide appropriate countermeasures. The emphasis is on personal and workplace practices which will limit the risk of individuals being exploited as an attack vector.

2) Target group: All employees including new employees, contractors and, in some instances, third-party service providers.

3) Objectives**:** After completing the awareness, individuals will be able to

- Identify basic cyber threats, risks and opportunities,
- employ sound personal and workplace cyber security practices,
- be aware of critical organisational assets,
- be aware of the exploitation of the human element as attack vector,
- understand policies and procedures to secure information systems, and
- understand and recognise countermeasures.

4) Overview of core content

- Cyber risks, cyber threats and cyber attacks,
- concepts of Intelligence, CI and CCI,
- organisational policies and procedures,
- insider threat,
- techniques used by cyber actors,
- data security and privacy,
- personal security,
- computer and mobile security, and
- internet and email security.

5) FCCI: Calibration and pitching

Our FCCI can be used as follows to select and calibrate content pitch at the awareness level:

Table 9: Application of the FCCI in designing CCI awareness (Author)

			LEVEL									
FCCI BUILDING BLOCKS	**#**	**CONTENT**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	1	Theory										
	2	Organisation										
	3	Intelligence										
	4	Counterintelligence										
	5	Cyber CI										
	6	CCI Matrix										
	7	Delineation										
	8	CCI Process										

6) Delivery methods and techniques.

Several methods or techniques can be used to deliver an awareness programme, namely classroom tuition, workshops, online courses, seminars and open lectures. Supplementary techniques include intranet postings, posters, videos, games, quizzes, etc. In this section we submitted a proposal on CCI awareness and now proceed with examining CCI fundamental training.

14.3.4.2 CCI Fundamental Training (See Tier 2 – Figure 43)

CCI training, to reiterate is essential for improving the effectiveness of the organisation in achieving its strategic objectives. Training addresses employee competencies (knowledge, skills and attitude), skills gaps, re-skilling and upskilling. Training programmes are structured according to proficiency levels (fundamental, functional and

advanced – see Figure 43) and customised, where relevant, as *per* the requirements of functions or roles.

CCI fundamental training is at an entry level and provides functionaries with a sound, but not necessarily detailed, CCI knowledge. It is aimed at those with direct/indirect CCI responsibilities or those requiring an organisational CCI background for other organisational functions. Since CCI is multi-disciplinary, fundamental training should transfer a sound grasp of CCI as subset of CI and intelligence. It should also convey the CCI modes of active-offensive, active-defensive, passive-offensive and passive-defensive.

The key elements of CCI functional training can be summarised as follow:

1) Description: A blended cyber security and CI training that is a bridging programme between CCI awareness and CCI functional training. This level covers a fundamental understanding of CCI skills, computer hardware, - software, - networks and- systems. It addresses both offensive and defensive dimensions.

2) Target groups: Functionaries with direct/indirect CCI responsibilities, those wanting to enter the CCI realm or requiring an organisational CCI background to effectively fulfil other organisational functions.

3) Objectives**:** After completing fundamental training, individuals will

- Be equipped with knowledge, skills and tools to counter cyber threats,
- have a grasp of CI and CCI's history with a view on instilling a professional 'self-awareness', [16]
- understand software security, networks security and systems security vulnerabilities,
- understand and be able to apply software security, networks security and systems security measures, and
- have been introduced to basic offensive and defensive CCI, cyber warfare and CCI strategies.

[16] See in Caelli, Liu and Longley (2013) as cited in Section 3.2 (Chapter 3). Practically such a history and professional 'self-awareness' will be included in Building Block 1: Theory.

4) Overview of content

- Information technology security (computer security, networks security, data security),
- physical security,
- cyber threat landscape,
- cyber actors and attack vectors,
- cyber intelligence (cyber collection) and deception,
- social media and its role to cyber collection, threats and attacks,
- policies, procedures and standards (CI, CCI information and cyber security),
- fundamentals of aspects such as penetration testing, cryptography, digital forensics, and
- cyber resilience or cyber risk management based approach.

5) FCCI: Calibration and pitching

Our FCCI can be used as follows to select and calibrate content pitch at the awareness level:

Table 10: Application of the FCCI in designing fundamental CCI training (Author)

			LEVEL									
FCCI BUILDING BLOCKS	**#**	**CONTENT**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	1	Theory										
	2	Organisation										
	3	Intelligence										
	4	Counterintelligence										
	5	Cyber CI										
	6	CCI Matrix										
	7	Delineation										
	8	CCI Process										

6) Delivery methods and techniques

Several methods or techniques can be used to deliver a fundamental programme, namely classroom tuition, online, hands-on or virtual and practical exercises.

14.3.4.3 CCI Functional Training (See Tier 3 – Figure 43)

CCI functional training is at an intermediate level. It is a role-based training because it is structured according to the functions and responsibilities of specific CCI occupational domains. Such occupational domains could include (but are not limited to): CCI Investigations, CCI Analysis, CCI Collection, CCI Deception Operations, CCI Technical Specialisation (Black 2014; Jaquire, Duvenage & von Solms 2018). The design and development of the training curriculum will differ according to specific skills as required by a particular role. In addition, each occupational domain has further areas of specialisation and/or progressions. CCI Analysis would, for example, be performed by technical-tactical – , operational – and strategic analysts. While analysts share a common skillset, there are simultaneously unique skills demanded on each of these levels, namely: technical/tactical –, operational –- and strategic.[17] Consequently, each different level of CCI Analysis requires customised training. For illustration purposes this subsection uses strategic CCI Analysis to illustrate the FCCI's application (See Table 11 on the next page).

Description: A blended CCI technical and CI training that builds on the knowledge and skills acquired in the fundamental CCI training. This training is structured according to the functions and responsibilities of specific CCI occupational domains. .

1) Target group: The training for CCI workforce and all functions in both CCI offensive and defensive domains.

2) Objective: After completing the awareness, individuals will be equipped with knowledge, skills, attitude and tools to conduct CCI functions according to a specific domain.

[17] See Table 7, Chapter 11 for more detail.

3) Overview of content

Although topics and pitching vary significantly between, and within, occupational domains, the following (predominately technical aspects) will usually be included in training for all domains:

- Cyber threat intelligence,
- collection (OSINT, CYBINT,HUMINT & SOCMINT),
- digital forensics, malware analysis and reverse engineering
- advanced networks,
- cryptography,
- vulnerability assessments, penetration testing and hacking,
- exploitation and deception,
- data analytics and incident response management, as well
- cyber intelligence and counterintelligence analysis,

4) FCCI: Calibration and pitching

For illustration purposes this subsection uses strategic CCI Analysis to illustrate the FCCI's application :

Table 11: Application of the FCCI in designing functional training for CCI strategic analysis (Author)

			LEVEL									
FCCI BUILDING BLOCKS	**#**	**CONTENT**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	1	Theory										
	2	Organisation										
	3	Intelligence										
	4	Counterintelligence										
	5	Cyber CI										
	6	CCI Matrix										
	7	Delineation										
	8	CCI Process										

5) Delivery methods and techniques

There are many methods or techniques for delivering a functional training programme such as classroom, online, hands-on or virtual practical, cyber games, emulation and simulation exercises (blue team, red team), research – and project-based assignments.

14.3.4.4 CCI Advanced Training (See Tier 4 – Figure 43)

This training proficiency level equips individuals with relevant specialist knowledge and skills. According to Toth & Klein (2013), this level "integrates training, education and experience with an assessment mechanism to validate knowledge and skills, resulting in the 'certification 'of a predefined level of competence". For a certain part, this level of CCI training will thus draw on industry-based knowledge. Serving as examples are the training and assessment conducted by external certification bodies such as the EC-Council, ISACA, (ISC)², SANS and CompTIA.

Within statutory state security structures internationally, however, external industry-based training is complemented by advanced in-house training in especially CCI's offensive dimensions. Given its specialized nature, this offensive CCI training is typically provided in small group and one-on-one format. It usually progresses from emulation and simulation exercises to 'real world' adversary engagement of as part of an experienced CCI team. This being an unclassified thesis, advanced CCI training are not further elaborated upon. The following application of the FCCI in Table 12 (next page) gives and high-level indication of advanced training's calibration:

Table 12 follows on the next page

Table 12: Application of the FCCI in advanced CCI training (Author)

			LEVEL									
FCCI BUILDING BLOCKS	**#**	**CONTENT**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	1	Theory										
	2	Organisation										
	3	Intelligence										
	4	Counterintelligence										
	5	Cyber CI										
	6	CCI Matrix										
	7	Delineation										
	8	CCI Process										

In this section we advanced a high level proposition a CCI ATP. This proposition consists of a four-tiered model which ranges from CCI awareness (Tier 1) to Advanced CCI training (Tier 4). The next section concludes the chapter and this part of the thesis.

14.4 CONCLUSION

Part 4 of the thesis, which comprises Chapter 14, aimed to illustrate the FCCI as a conceptual construct practically useful to an organisation's CCI Awareness and Training Programme (ATP). To this end we first provided context on the broader concept of CCI Awareness, Education and Training (AET) and its complexities. We proceeded with positioning CCI Awareness and Training Programme (ATP) as a subset of CCI AET. The generic organisational CCI ATP we then advanced consisted of a four-tiered model which we depicted graphically and discussed narratively. As part of this proposition we illustrated our FCCI as tool useful for selecting training content and calibrating training pitch. In so doing , we validated the thesis' central hypothesis on a credible an practically useful FCCI which explain what CCI is and how it 'works'.

PART 5

EVALUATION AND CONCLUSION

Part 5 evaluates the problem statement, research questions and hypothesis are evaluated, and areas for further research on CCI are highlighted. It consists of **Chapter 15**.

CHAPTER 15
EVALUATION AND CONCLUSION

15.1 INTRODUCTION

In this chapter, we conclude the thesis by addressing the following:

- Section 15.2: Research context
- Section 15.3: Evaluation of the problem statement, research questions, hypothesis and research objective
- Section 15.4: Observations on the significance of the research
- Section 15.5: Limitations and suggestions on further research
- Section 15.6: Conclusion

15.2 RESEARCH CONTEXT

This study was prompted by the challenges posed by the cyber threatscape which necessitates an integrated cybersecurity approach with CCI at its core. Sophisticated threats, we argued, increasingly have intelligence actions (such as espionage) as an essential feature. In Chapter 1, we emphasised the centrality of CCI in effectively engaging morphing high-end cyber threats. We asserted that CCI is central to coherently and proactively meeting these threats. Although only well-resourced entities can afford fully-fledged capacity in this field, a CCI mindset and approach could also benefit smaller organisations.

Effective practice, however, requires good theory. We emphasised that conceptual models and frameworks are not 'nice to have' academic toys. Theory conditions our thinking and our approach to practice. What we therefore need for CCI is a sound overarching construct such as a framework. Throughout the thesis, we demonstrated academic theory and practice as two sides of the same coin. On an academic level, a framework has to consolidate and direct CCI research. On a practical level, a framework must serve as a template for performing CCI work in practice. On both accounts, we asserted, a framework is an idealisation – it is an aimpoint of what CCI should look like when everything goes as planned.

In this section, we discussed the research context of this study. We now proceed with an appraisal of the problem statement, research questions, hypotheses and research objective.

15.3 EVALUATION OF PROBLEM STATEMENT, RESEARCH QUESTIONS, HYPOTHESIS AND RESEARCH OBJECTIVE

The introduction to this thesis (Section 1.1 of Chapter 1) as well as Chapter 2, showed the academic and practical importance of a conceptual FCCI. Yet, as far as we could ascertain, such framework is lacking in the consulted literature.

15.3.1 RESTATEMENT OF THE PROBLEM STATEMENT, RESEARCH QUESTIONS, HYPOTHESES AND RESEARCH OBJECTIVE

Flowing from this void in the literature reviewed, we formulated the study's primary **problem statement** in Chapter 1 (Section 1.2) as follows:

> "From the literature studied, no overarching conceptual CCI framework that can provide a premise for establishing CCI as an academic subdiscipline, a topic of instruction and a research field could be found."

Based on the primary research question, the **central research questions** of the study posed (Section 1.2 of Chapter 1) were:

> "What academically credible conceptual framework can be advanced to notionally structure CCI?
>
> What should the features and components of the framework be, and how should they be configured?"
>
> Can conceptual constructs derived from Intelligence Studies (notably statutory intelligence and counterintelligence) be usefully applied to CCI and thus to the FCCI's design?

In response to the research question, we advanced the following **hypotheses** to direct the study (Section 1.3 of Chapter 1):

> "The thesis's central **hypothesis** is that an FCCI can be designed by means of an inductive, qualitative methodology. By postulating the critical

notional constructs which comprise CCI and by outlying the constructs' relations, the framework can credibly explain what CCI is and how it 'works'.

Accompanying the central hypothesis, the thesis' **two secondary hypotheses** were:

"Criteria can be formulated to derive the FCCI's features, components and configuration.

Conceptual constructs from Intelligence Studies can be applied to CCI and utilised for the FCCI's design. "

We concretised the hypotheses in the study's **primary objective** which read as follows:

"The study's primary objective is to construct the FCCI as a conceptual framework for notionally structuring CCI as an emerging, multidisciplinary field of enquiry.

This construction will follow an inductive qualitative methodology within the realist paradigm and will include an evaluative literature study to develop the FCCI and its components."

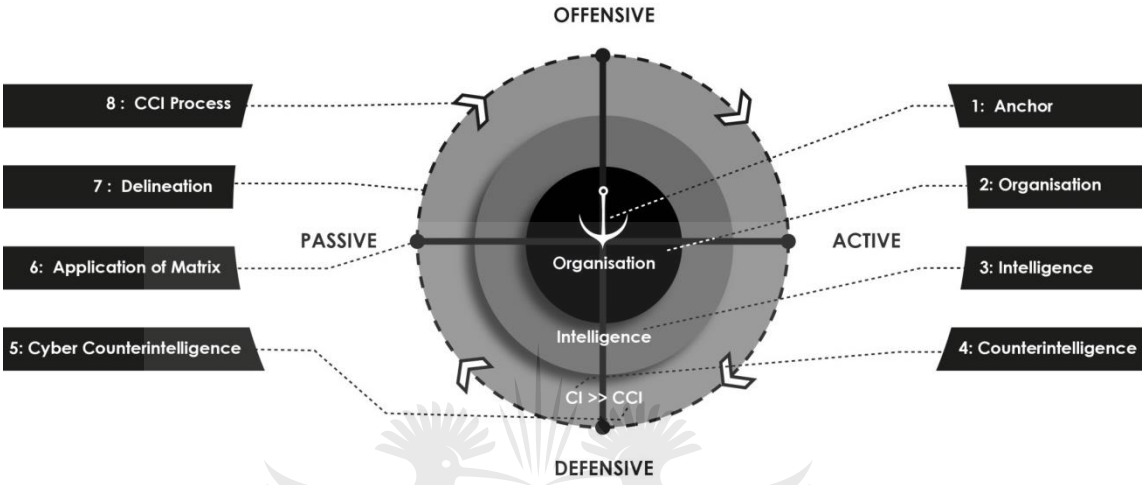
15.3.2 EVALUATION OF PART 1 (CHAPTERS 2 AND 3)

To test the **hypotheses** and pursue the **primary objective**, we proceeded by laying the foundation for the construction of our FCCI. To this end, in Chapter 2 we identified the features with which an academically credible FCCI should comply. This chapter's outcome validated the **secondary hypothesis**, which reads "criteria can be formulated to derive the FCCI's features, components and configuration" (Section 1.3 of Chapter 1).

We subsequently conducted an evaluative literature review (Chapter 3). This corroborated our **problem statement** on the absence of an FCCI (in the consulted sources) and provided elements useful to constructing the FCCI in subsequent chapters. Chapter 3 was therefore in line with the quantitative methodology (inclusive of an evaluative literature review) referred to in the **primary objective** and the **central hypothesis**.

15.3.3 EVALUATION OF PART 2 (CHAPTER 4)

To guide the reader to the actual construction of our FCCI, in Chapter 4 we provided a high-level blueprint and road map. This preview consisted of a graphical representation and a concise narrative overview of the integrated FCCI and its building blocks. The FCCI was graphically depicted in this chapter as follows:



Since Chapter 4 is a preview of Chapters 5 to 13 (Part 3), its evaluation concurs with the assertions made per 'Evaluation of Part 3' (i.e. directly following Subsection 15.3.4).

15.3.4 EVALUATION OF PART 3 (CHAPTERS 5–13)

Part 3, comprising Chapter 5 -13, constituted the thesis' core. For purposes of Part 3's evaluation, we appraise the central hypothesis and the secondary hypotheses separately.

15.3.4.1 Evaluation: Central Hypothesis and Research Objective

In Part 3(of the thesis, we proceeded with a step-by-step construction of our FCCI. This step-by-step construction consisted of eight sequential building blocks, the "critical notional constructs" we mentioned in the **central hypothesis**. We derived these building blocks by using the inductive qualitative methodology referred to in the **objective** and the **central hypothesis**.

Throughout the thesis, we highlighted the academic and practical utility of each building block. In line with our **central hypothesis,** we discussed not only the building blocks but also the "relations" between them. This was done to test the hypothesis' contention that an FCCI so constructed will explain "what CI is and how it 'works'".

To explain **what CCI is**, we:

- Showed CCI as a micro-theoretical construct and positioned the FCCI as part of academic theory (Chapter 5)
- Explained CCI as intricately linked to and part of the organisation as well the intelligence and CI endeavour (Chapters 6–8)
- Defined CCI (Chapter 9)
- Included a specific building block to delineate CCI (Chapter 12)

Concurrently with explaining what CCI is, we explored our **central hypothesis'** assertion on **how CCI 'works'**. In this regard, we:

- Showed the interface between CCI on the one hand and the organisation, intelligence and CI on the other hand. We explained CCI as a CI subset and its practical execution as being determined by the organisation's goals, strategy and intelligence endeavour (Chapters 6–8).
- Provided a high-level overview of CCI tools (Chapter 9).
- Advanced a CCI matrix which (1) synchronises CI and CCI tools, (2) aids the configuration of a CCI posture in accordance with the organisation's needs and (3) describes the levels on which CCI is executed. Furthermore, the CCI matrix's 'working' was illustrated by means of a case study.
- Provided a CCI process model which describes the sequential steps of performing CCI.

Throughout Chapters 5 to 13, we presented the FCCI as a notional framework to structure CCI. Therefore, the aspects covered in our FCCI range from abstract theory (Chapter 5) to specific CCI tools and processes (Chapters 9-11 and 13). In doing so, we achieved the **primary aim** to "construct the FCCI as a conceptual framework for notionally structuring CCI".

15.3.4.2 Evaluation: Secondary Hypotheses

The thesis **secondary hypothesis** that "**criteria** can be formulated to derive the FCCI's features, components and configuration" was already substantiated in Chapter 2 (part 1). Nonetheless, the construction of a FCCI (in Chapters 5 to 13) that explains what CCI is and 'how it works' further validates this secondary hypothesis.

The thesis' other secondary **hypothesis,** namely that **conceptual constructs from Intelligence Studies** can be applied for the FCCI's design, was convincingly validated

throughout Chapters 5 to 13. Such concepts varied from the 'abstract' theoretical (e.g. positivist, realist positioning) to the more concrete (e.g. the CI process applied to CCI).

15.3.5 EVALUATION OF PART 4 (CHAPTER 14)

Part 4 illustrated the FCCI as a conceptual construct practically useful to an organisation's CCI Awareness and Training Programme (ATP). Within the context of a CCI ATP, the FCCI was applied as a tool to convey what CCI is and how it 'works' – thus corroborating the **central hypothesis**. Since the FCCI was shown as useful to CCI training, Chapter 14 by extension also validated the **secondary hypotheses** on design criteria and the application of Intelligence Studies' concepts.

15.3.6 SUMMARISED EVALUATION

As is clear from the above, the research we conducted validated the central hypothesis and achieved the **research objective** of designing a framework that explains what CCI is and how it 'works'. By following an inductive, qualitative methodology, we constructed our FCCI by forwarding building blocks (critical notional constructs) and showing their interaction. The FCCI's construction was guided by a set of derived criteria (secondary hypothesis) and build on concepts from Intelligence Studies (secondary hypothesis. Since we validated the **hypotheses** and achieved the aim of the study, we succeeded in addressing the study's **problem statement** and **research questions**.

15.4 OBSERVATIONS ON THE SIGNIFICANCE OF THE RESEARCH

The attainment of the research objective does of course not necessarily imply that the thesis comply with the requirements for a doctoral thesis. In line with international best practice, the University of Johannesburg (2018b) requires of a doctoral thesis to make "a significant and original contribution to the body of knowledge in the discipline or field." The following three information sets support the notion that thesis, and the FCCI it advances, constitutes a **credible, significant and original contribution** to the field:

- Subsection 15.4.1: Methodology and approach
- Subsection 15.4.2: Extensive peer-review and positive feedback
- Subsection 15.4.3: Utilisation of research by other scholars and institutions

We are aware of the fact that previous chapters referred to FCCI research's significance and the use thereof by other academics/institutions (notably Chapter 1, Chapter 3 and Chapter 10). For purposes of this section, excessive referencing to these chapters would have inconvenienced the reader and distracted from the reading experience. **Therefore, in the interest of easier reading, the discussion of our FCCI research's significance in this section will to some degree overlap with previous chapters.** For the reader's convenience, we also recapitulate contextual information on, for example, the Mitre Corporation and Utica College. With these qualifications we now proceed with discussing the three information sets supporting the assertion of the thesis constituting a credible, significant and original contribution to the field

15.4.1 Methodology and approach

The FCCI can be deemed credible since its conceptualisation, design and construction followed an academically sound inductive, qualitative methodology. The FCCI's overall design and was guided by criteria derived through extensive multidisciplinary research (Chapter 2). In addition, a comprehensive literature study (Chapter 3) not only informed our FCCI's design and construction (Chapters 4-13), but – as was mentioned earlier – also convincingly substantiates the assertion of the FCCI being a **significant and novel contribution** to the field. The veracity of the literature review and assertions made therein, were confirmed by the successful peer-review of the work at the *17th European Conference on Cyber Warfare and Security* (Duvenage, Jaquire & von Solms 2018a). The organisers ranked the literature review as one of the conference's best papers and an expanded version thereof was invited for publication by the *Journal of Information Warfare* (Duvenage, Jaquire & von Solms 2018b).

Furthermore, care was taken throughout the thesis to argue the **academic and practical significance** of not only the integrated FCCI, but also each of its building blocks.

15.4.2 Peer-review and feedback

The integrated FCCI and its respective building blocks were subjected to extensive peer review. A total of **eight papers** were presented and subsequently published in the proceedings of leading international conferences (Annexures A, B, D, E, F, G, I, J). Feedback received from peer-review panels was overwhelming positive and confirmed the FCCI and aspects thereof as an **original** and/or **significant contribution** to the field. In addition, **two articles** were published in a highly regarded international journal, namely the *Journal of Information Warfare* (Annexures C and H). A further **two papers**

were successfully submitted for peer-review and subsequently accepted for presentation at the 18th European Conference on Cyber Warfare and Security in July 2019 (Annexures K and L).

The above noted peer-review on the FCCI's research significance was further corroborated by expert opinions during a University of Johannesburg benchmarking process which involved seasoned cybersecurity and intelligence practitioners. Remarking on the FCCI's significance and originality, one of the experts stated (University of Johannesburg 2018c):

> [This research] ... not only consolidates the meagre existing knowledge on the applicable field (i.e. CCI), but also, and more pertinently creates new knowledge … The real value of the research lies in the conceptualisation of a proposed Conceptual Framework. Not only is this unprecedented, but it will also take the academic pursuit of CCI forward by leaps and bounds.

In addition to academic peer-review, key aspects of the FCCI were included in papers/presentations on CCI at pre-eminent, non-academic events attended by IT executives and practitioners (See Chapter 1, Section 1.6). Hosts of conferences utilised to benchmark our FCCI research included authoritative entities such as ISACA, (ISC)^2 and IT Web. Also in this instance, the feedback received affirmed the FCCI's significance and novelty.

15.4.3: Utilisation of research by other academics and institutions

In addition to peer-review feedback, the utilisation of research by others could be used as an indication of an academic study's credibility, significance and originality. Such use is *inter alia* reflected in citations and references. Citations and referencing rates are significant influenced by the nature of the particular study field and the academic interest it attracts. In this regard, note should be taken of CCI status as an emerging specialised subdiscipline with the already niche of area of CI (Prunckun 2018; Stech & Heckman 2018). Internationally, nation states' security structures generate a voluminous body of classified CI material. In the public and academic domain, however, CI "remains little known or understood" (Van Cleave 2007, Prunckun 2014). Chapters 1 and 3 observed on the surprisingly few works in the public domain which explain CI's theory and practice (Prunckun 2012, Prunckun 2014, Van Cleave 2007, Duvenage 2011). Consequently, and in comparison with other Intelligence Study fields, citations of even general, authoritative works on CI are far less prolific (c*f*. Prunckun 2014, Van

Cleave 2007). Within the young, emerging and specialised subdiscipline of CCI this is all the more so (Stech & Heckman 2018). Thus, for now, the key measure for CCI citations and referencing is **rather the 'who'** (i.e. person/ institution citing) **than the 'how many'** (i.e. number of citations).

- Within the context provided in the preceding paragraph, the following non-exhaustive examples attest to the FCCI research presented in this thesis as being a credible, **original and significant contribution** to the study field: The **Mitre Corporation** is a prominent US federally funded institution with an estimated revenue of $1.4 billion (Bloomberg 2018). Branching out from their world-leading work on cyber denial and deception, Mitre researchers have recently been focusing on CCI (Stech & Heckman 2018). Flowing from this research, Stech and Heckman (2018) postulated a CCI framework for "active cyber defense". This postulation extensively cites, incorporates, and further develops, concepts we originally advanced in our FCCI research. [18] With reference to our FCCI research's significance, Stech and Heckman (2018) state: "[The] researchers are providing increasingly detailed concepts for implementing CCI in enterprises. We recommend such concepts, combined with cyber denial and deception, to cyber defenders."
- The US-based **Utica College** offers CCI as a post-graduate specialisation field. Utica holds designations of academic excellence from the US National Security Agency, the Department of Defense as well as the Department of Homeland Security (Utica 2018). In a recently completed Master of Science project completed at this college, Justiniano (2017) draws on several elements we advanced in the research leading up to this thesis. Justiniano (2017) describes our FCCI research as "perhaps the best effort towards academically framing and formalizing CCI to date".
- Five FCCI research papers (Duvenage & von Solms 2014; Duvenage, von Solms & Corregidor 2015; Duvenage, Jaquire & von Solms 2016, Jaquire, Duvenage & von Solms 2018, Sithole *et al* 2019) incorporated in this thesis, appear on the recommended reading list of the prestigious **US Naval War College** (2018a, 2019). The US Naval War College was established in 1884 and has, according to its website, "trained more than 24,000 U.S. and international

[18] For more detail please see Section 3.7 (Chapter 3)

military officers and hundreds of federal civilian executives across its six colleges and various academic centers." (US Naval War College (2018b)

- A research stream at the **University of Johannesburg** (UJ), to recapitulate, aims to develop a CCI maturity model with emphasis on governments and non-state actors in emerging countries (University of Johannesburg 2018a). Our FCCI research is widely cited in the three internationally peer-reviewed research papers (Jaquire & von Solms 2017 a-c) and a recently completed doctoral thesis (Jaquire 2018) that flowed from this research stream.
- An article featured in the **Italian** government's **Intelligence and Internal Security Agency**'s public magazine contains extensive narrative and graphical extracts from our FCCI research (Teti 2016).
- Our FCCI research was cited in a journal article by an academic associated with the **Peoples' Republic of China's (PRC)** state security structures (Huang 2015).

This section provided context for assessing the significance and originality of the research contained in the thesis. We now proceed with observations on research limitations.

15.5 LIMITATIONS AND SUGGESTIONS ON FURTHER RESEARCH

As was expected from the outset, the study's primary challenge pertained to limitations in CCI-focused literature available for an unclassified thesis. While CCI is practised and taught by various governments' security apparatus, such material is not publically available. Nonetheless, the limited but growing body of academic, peer-reviewed CCI research provided insights valuable to the FCCI's design. Furthermore, and also in line with expectations, concepts derived from Intelligence Studies' literature proved useful to the FCCI's construction. However, within the confines of a high-level theoretical framework only scant reference was made to academic disciplines and fields other than Intelligence Studies

The FCCI we advanced in this thesis was thus qualified as a skeletal framework (Subsection 2.2.2 of Chapter 2). Consequently, both the overall FCCI and its respective building blocks can admittedly benefit substantially from further research. With more rigorous and detailed research, the conceptual **FCCI** can be developed into a **CCI model**.

Although it is not possible to fully illustrate the outcomes of our FCCI's application within the confines of this thesis, several major and recent cyber breaches affirm the framework's its 'real-world' utility. **Case studies** of such incidents will be central to evolving the FCCI into a CCI model and are thus proposed as an area for further research.

In respect of both theorisation and case studies, a foremost priority item on the research agenda ought to be the interface and dynamics between **CCI and information/cyber warfare**. Currently, even outstanding works on information and cyber warfare make scant reference to CCI and *vice versa* (See Section 1.1, Chapter 1 as well as Section 3.5 – 3.7, Chapter 3). This near void presents fertile, yet conceptually intricate, ground for further research. It is hoped that the FCCI will provide a 'scaffold' for CCI to benefit academically from the rich and expansive body of literature focused on information and cyber warfare.

Earlier in this section and at various other junctures in the thesis (e.g. Subsection 2.2.3 of Chapter 2 and Subsection 12.3.2 of Chapter 12), we mentioned that CCI is a multifaceted subject that ought to benefit from inputs from various academic disciplines. These disciplines include, to name a few, Intelligence Studies and International Relations (both part of Political Science), Computer Science and Informatics, Business Studies, Sociology, Psychology, Law, Linguistics and History. In Chapter 3 (Section 3.2), for example, we noted that to be truly professional, "practitioners must clearly understand that discipline's history" (Caelli, Liu & Longley 2013). The importance of such a history for a field as young as CCI can thus hardly be overemphasised and it was further highlighted in Chapter 14, Section 14.3.4.2. In a similar vein, the other academic disciplines cited are their own particular relevance to CCI. Being a multi-faceted field, CCI cannot be demarcated rigidly; instead it is "a mosaic of overlapping academic interests" (Subsection 12.3.2 of Chapter 12). To advance CCI as an academic field, one of the items on the CCI research agenda has to be identifying and describing these 'overlaps'. This will provide pointers to the respective contributions the aforementioned academic disciplines can make to, and benefit from, developing multidisciplinary CCI.

15.6 CONCLUSION

This thesis showed CCI as an academic subdiscipline in its infancy with the agenda for its development in various respects unclear. Nonetheless, the budding body of

academic literature, which has been expanding over a short period of time, is showing great promise. We advanced a tentative conceptual framework (FCCI) to aid CCI's academic evolvement. However, the FCCI and its building blocks could not be explicated in detail within the confines of a thesis. Only the essential contours of, and rationale behind, the FCCI's design were therefore provided. The FCCI was qualified as an exploratory postulation, hopefully constructive to practice and academic discourse.

The FCCI is by its very nature a contestable academic construct. What is not contestable is the importance and practical significance of academic theory in meeting the demands posed by a threat landscape in which intelligence actors of various types continue to predominate.

PART 6

REFERENCES AND ANNEXURES

REFERENCES

Amankwa, E., Loock, M., & Kritzinger, E. (2014). 'A conceptual analysis of information security education, information security training and information security awareness definitions' in *9th International Conference for Internet Technology and Secured Transactions* (ICITST-2014): 248-252.

Armistead, E. L. (2010) *Information Operations Matters: Best Practices*, Potomac Books, Dulles, US.

Armistead, L. (ed.) (2004) *Information Operations: Warfare and the Hard Reality of Soft Power*, Potomac Books, Washington, D.C., US.

Andress, J. & Winterfeld, S. (2014) *Cyber warfare – techniques, tactics and tools for security practitioners*, second edition, Elsevier, Waltham, US.

Bardin, J. (2011) 'Ten commandments of cyber counterintelligence', *CSO Magazine* (online), accessed on 09/01/2013 at http://www.csoonline.com/article/ 2136458/identity-management/ten-commandments -of-cyber-counterintelligence.

Berkowitz, B.D. & Goodman A.E. (2000) *Best truth: Intelligence in the information age,* Yale University Press, New Haven, United States of America (US).

Bernhardt, W.A. (2003) *A qualitative conceptual framework for conducting risk and threat assessment in the South African domestic intelligence environment*, unpublished DPhil thesis, University of Pretoria. Pretoria, South Africa.

Betts, R.K. (2004) 'Analysis, war, and decision: Why intelligence failures are inevitable' in Johnson, L.K. & Wirtz, J.J. (eds) *Strategic intelligence: Windows into a secret world (an anthology),* Roxbury Publishing Company, Los Angeles, US.

Black, J. M. (2014). *The complexity of cyber counterintelligence training*, unpublished master's dissertation, Utica College, New York, US.

Bloomberg (2018) *Company Overview of the MITRE Corporation*, accessed on 24/08/2018 at https://www.bloomberg.com/research/stocks/private/snapshot.asp ?privcapId=4198312.

Boawn, D.L. (2014) *Cyber counterintelligence, defending the United States' information technology and communications critical infrastructure from Chinese threats*, unpublished master's dissertation, Utica College, New York, US.

Bodmer, S.A. *et al.* (2012) *Reverse deception – Organized cyber threat counter-exploitation*, McGraw-Hill, New York, US.

Brouard, F. (2004) 'Business intelligence for Canadian corporations after September 11', in *Journal of Competitive Intelligence and Management*, 2(1):1–17.

Bruneau, T.C. & Dombroski, K. (2004) *Reforming intelligence: The challenge of control in new democracies,* US Naval Postgraduate School, accessed on 16/03/2008 at http://www.ccmr.org/public/library_file_proxy.cfm/lid/5258 .

Buchanan, B. (2016) *The cybersecurity dilemma – Hacking, trust, and fear between nations*, C. Hurst & Co. Publishers, London, United Kingdom (UK).

Caballero, A. (2017) 'Information security essentials for information technology managers: protecting mission-critical systems' in J. R. Vacca (ed.), *Computer and Information Security Handbook*, third edition, Morgan Kaufmann (Elsevier).

Caelli W., Liu V. & Longley, D. (2013) 'Background to the development of a curriculum for the history of "cyber" and "communications security" ' in Dodge R.C. & Futcher L. (eds.) *Information Assurance and Security Education and Training*, IFIP Advances in Information and Communication Technology, vol. 406, Springer, Berlin, Germany.

Campen, A.D., Dearth, D.H. & Godden, R.T. (eds.) (1996) *Cyberwar: Security, Strategy, and Conflict in the Information Age*, AFCEA International Press, Fairfax, US.

Carrol, J. (2009) 'Cyber counter intelligence' in *Defense Tech*, accessed on 03/12/2012 at http://defensetech.org/2009/03/09/counter-cyber-intelligence/ .

Chismon, D. & Ruks, M. (2015) *Threat intelligence: Collecting, analysing, evaluating*, MWR Infosecurity, UK.

Clarke, R. A. & Knake, R. (2010) *Cyber War: The Next Threat to National Security and What to Do About It*, Harper-Collins, New York, US.

Clarke, R.M. (2004) *Intelligence analysis: A target-centric approach*, CQ Press, Washington D.C., US.

Codevilla, A. (1992) *Informing statecraft – Intelligence for a new century*, The Free Press, New York, US.

Coats, D.R. (201) *Worldwide threat assessment of the US Intelligence Community February 13, 2018,* accessed on 27/07/2018 at https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Crampton, J. *et al.* (2006) 'Information security' in Gill, M. (ed.) *The handbook of security*, Palgrave Macmillan, London, UK.

CrowdStrike (2016) *Global Threat Report 2015*, accessed at http://www.crowdstrike.com/global-threat-report-2015/

Davey, J. & Armstrong, H (2002) 'Dominating the attacker: Use of intelligence and counterintelligence in cyberwarfare' in *Journal of Information Warfare*, 2(1):23–31.

Denning, D.E. (1999) *Information warfare and security*. Addison-Wesley, Boston, US.

De Vos, A.S. (2006) 'Scientific theory on professional research' in De Vos, A.S. *et al.* (eds). *Research at grass roots for the social science and human science professions*, 3rd Edition, Van Schaik Publishers, Pretoria, South Africa.

de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998, April). *NITS: Information technology security training requirements: a role- and performance-based model*, National Institute of Standards and Technology, Computer Information Resource Centre, retrieved 09 2018, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

Dtex (2017). 2017 *Insider Threat intelligence report*. retrieved 18 October 2017, from Dtex Systems: https://www.dtexsystems.com/2017-insider-threat-intelligence-report/

Duvenage, P.C. & Hough, M. (2011) 'The conceptual structuring of the intelligence and the counterintelligence processes: Enduring holy grails or crumbling axioms – *Quo vadis*?' in *Strategic Review for Southern Africa*, 33(1):29–77.

Duvenage, P.C. (2011) *Open-source environmental scanning and risk assessment in the statutory counterespionage milieu*, unpublished D.Phil. thesis, University of Pretoria, Pretoria, South Africa.

Duvenage, P.C. (2013) 'Counterintelligence' in Prunckun, H. (ed.), *Intelligence and private investigation: Developing sophisticated methods for conducting inquiries,* Charles C. Thomas Publishers, Springfield, Illinois, US.

Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2016) 'Conceptualising cyber counterintelligence – Two tentative building blocks' in *Published Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, Germany, June.

Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2018a) 'A selective literature review on cyber counterintelligence' in *Published Proceedings of the 17th European Conference on Cyber Warfare and Security*, Oslo, Norway, June.

Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2018b) 'Towards a literature review on cyber counterintelligence' in *Journal of Information Warfare*, 17(4), 11-25.

Duvenage, P.C., Jaquire, V. J. & von Solms, S.H. (2019) 'A cyber counterintelligence matrix for outsmarting your adversaries' in *Published Proceedings of the 18th European Conference on Cyber Warfare and Security*, Coimbra, Portugal, July.

Duvenage, P.C., Sithole, T.G. & von Solms, S.H. (2017) 'A conceptual framework for cyber counterintelligence – Theory that really matters!' in *Published Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland, June.

Duvenage, P.C. & von Solms. S.H. (2013) 'The case for cyber counterintelligence' in *Published Proceedings of the 5th International Workshop on ICT Uses in Warfare and the Safeguarding of Peace*, Institute of Electrical and Electronic Engineers (IEEE), Pretoria, South Africa, November.

Duvenage, P.C. & von Solms, S.H. (2014) 'Putting counterintelligence in cyber counterintelligence' in *Published Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece, July.

Duvenage, P.C. & von Solms. S.H. (2015) 'Cyber counterintelligence: Back to the future' in *Journal of Information Warfare*, 13(4):42–56.

Duvenage, P.C., von Solms, S.H. & Corregedor, M. (2015) 'The cyber counterintelligence process – A conceptual overview and theoretical proposition' in *Published Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK, July.

The Economist 2015, Counter-intelligence techniques may help firms protect themselves against cyber-attacks, viewed 24 May 2016, <http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protectthemselves>.

Evron, G. (2014) *Cyber Counter Intelligence: An attacker-based approach*, Honeynet Project Workshop, May 2014, Warsaw, Poland, viewed 07 October 2017, <https://www.youtube.com/watch?v=lJC3c-jMALU>.

Farchi, J. (2012) 'Offensive counter-intelligence and cyberwarfare – A paradigm shift in information security' in *Information System Control and Audit Association (ISACA)*, accessed on 16/02/206 at http://www.isaca.org/Knowledge-Center/..../Post.aspx?List=ef7cbc6d%2D9997%2D4b62%2D96a4% .

Fieber, T. J. (2015) *The Iranian computer network operations threat to U.S. critical infrastructures*, Master of Science (capstone project), Utica College.

Ferguson C. J. (2012) *Increasing the effectiveness of U.S. counterintelligence: Domestic and international micro-restructuring initiatives to mitigate cyberespionage*, unpublished master's dissertation, US Naval Postgraduate School, California, US.

Firestone, A. (2015) 'Shifting paradigms: The case for cyber counter-intelligence' in *InformationWeek, a*ccessed at http://www.darkreading.com/operations/shifting-paradigms-the-case-for-cyber-counter-intelligence/a/d -id/1318929 .

Francq, A. (2000) 'The use of counterintelligence, security, and countermeasures' in Fleisher, F.S. & Blenkhorn D.L. (eds), *Managing frontiers in competitive intelligence*, Quorum Books. Westport, US.

French, G.S. & Kim, J. (2009) 'Acknowledging the revolution: The urgent need for cyber counterintelligence' in *National Intelligence Journal*, 1(1):71–90.

Friedman, J. & Bouchard, M. (2015) *Definitive guide to cyber threat intelligence*, accessed on 07/12/2015 at https://cryptome.org/2015/09/cti-guide.pdf.

Giles, L. (2002) *Sun Tzu on the art of war* (translation), Dover Publications, New York, US.

Gill, P. (2006) 'What is intelligence theory?' in Treverton, G.F. *et al*., *Toward a theory of intelligence – Workshop Report*, RAND Cooperation, accessed on 2008/02/14 at http://www.rand.org/pubi/larf/proceedings/2006/Rand-CF219.pdf .

Gill, P. & Phythian, M. (2006) *Intelligence in an insecure world*. Polity Press, Cambridge, UK.

Gilliam, B. P. (2017) *Threat Intelligence in support of cyber situation awareness,* Unpublished doctoral thesis, Walden University, Minnesota, US.

Godson, R. (2001) *Dirty tricks or trump cards – U.S. covert action and counterintelligence*, Transaction Publishers, New Brunswick, US.

Greenwald, A.G. (2012) 'There is nothing so theoretical as a good method' in *Perspectives – Psychological Science*, 7(2):99–108.

Harvard University (2018): *Certificate - Managing Risk in the Information Age*, course material, Office of the Vice Provost for Learning Advances (VPAL), Massachusetts, US.

Heckman, K.E., Stech F.J. , Thomas R.K. , Schmoker B & Tsow A.W. (2015) *Cyber denial, deception and counter deception – A framework for supporting active cyber defense*, Springer International Publishing, Cham, Switzerland.

Hough, M. (2006) 'The concept of national security strategy: The case of the United States and South Africa' in *Strategic Review for Southern Africa*, 38(2):1–18.

Huang, Z (2015) 分析了网络[illegible]提出在[illegible]

[illegible]

[illegible]

Hutchinson, B. & Warren, M. (2002) *Information Warfare: corporate attack and defence in a digital world,* Butterworth-Heinemann, Oxford, UK.

Hutchinson, W. & Warren, M. (2001) 'Principles of information warfare'*, Journal of Information Warfare Volume*, 1 (1): 1-6 IBM (2016) *2016 Cyber Security Intelligence Index,* accessed at https://www.ibm.com/security/data-breach/threat-intelligence-index.html .

Intelligence and National Security Alliance (INSA) (2011) *Cyber intelligence: Setting the landscape for an emerging discipline*, accessed at http://www.insaonline.org/I/d/a/Resources/Cyber_Intelligence.aspx.

INSA (2013) *Operational levels of cyber intelligence*, accessed at http://issuu.com/insalliance/docs/insa_wpcyberintelligence_pages_hir/16?e=6126110/4859250 .

INSA (2014a) *Operational Cyber Intelligence,* accessed at http://www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx .

INSA (2014b) *Strategic cyber intelligence*, accessed at http://www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx.

INSA (2015) *Tactical cyber intelligence*, accessed at http://www.insaonline.org/i/d/a/b/TacticalCyber.aspx .

Jabareen, Y. (2009) 'Building a conceptual framework: Philosophy, definitions, and procedure' in *International Journal of Qualitative Methods*, 8(4):49–62.

Janczewski, L.J. & Caelli, W. (2016) *Cyber conflicts and small states*, Routledge, New York, US.

Jaquire, V.J. (2018) *A framework for a cyber counterintelligence maturity model*, D.Com (Informatics) thesis, University of Johannesburg, Johannesburg, South Africa.

Jaquire, V.J., Duvenage, P.C. & von Solms, S.H. (2018) ' Building the CCI dream team' in *Published Proceedings of the 17th European Conference on Cyber Warfare and Security*, Oslo, Norway, June.

Jaquire, V.J. & von Solms, S.H. (2017a) 'Towards a cyber counterintelligence maturity model' in *Published Proceedings of the 12th International Conference on Cyber Warfare and Security*, Wright State University, Air Force Institute of Technology, Dayton, US, March.

Jaquire, V.J. & von Solms, S.H. (2017b) 'Developing a cyber counterintelligence maturity model for developing countries' in *Published Proceedings of the 2017 IST–Africa Conference*, Windhoek, Namibia, May–June.

Jaquire, V.J. & von Solms, S.H. (2017c) 'Cultivating a cyber counterintelligence maturity model' in *Published Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland, June.

Jones, A., Kovacich, G.L. & Luzwick, P.G. (2002) *Global information warfare*. Auerbach, Boca Raton, US.

Johnson, L.K. (ed.) (2007) *Strategic intelligence – The intelligence cycle: The flow of secret information from overseas to the highest councils of government*, Praeger Securities International, Westport, US.

Junghans, A. & Olsson, N. (2012) 'Does facilities management meet the requirements of an academic discipline?' in *Published Proceedings of the International Conference on Facilities Management,* Cape Town, South Africa, January.

Justiniano, J.E. (2017) *Advancing the capacity of a theater special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone*, Master of Science (capstone project), Utica College.

Kent, S (1949, 1966) *Strategic intelligence for American world policy*, Princeton University Press, Princeton, US.

Kim, J. S. (2018) *The Importance of Literature Review in Research Writing*. Available at https://owlcation.com /misc/literature_review

Kissel, R., & Wilson, M. (2010). 'Cyber security education, training, and awareness' in J. G. Voeller (Ed.), *Wiley handbook of science and technology for homeland security*, 4 Volume Set. John Wiley & Sons.

Knowles, J. A. (2013). *Applying computer network operations for offensive counterintelligence*, Master of Science (capstone project), Utica College.

Kopp, C. (2000) 'A fundamental paradigm of infowar', Systems, accessed on 2011/10/25 at http://www.ausairpower.net/OSR-0200.html.

KPMG (2013) *Cyber threat intelligence and the lessons from law enforcement*, accessed at http://www.kpmg.com/Global/en/IssuesAndInsights/Articles Publications/ Documents/cyber-threat-intelligence-final3.pdf .

Krishnan, A. (2009) *What are academic disciplines?* National Centre for Research Methods, University of Southampton, Southampton, UK.

Laksman, E (2013) *Realism and non-state actors revisited*, accessed at on 13 June 2018 at https://www.e-ir.info/2013/01/22/realism-and-non-state-actors-revisited/

Lee, R.M. (2014a) 'An introduction to cyber intelligence' in *Tripwire* blog series (1), accessed on 2015/01/04 at http://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/ .

Lee, R.M. (2014b) 'Developing your cyber intelligence analyst skills' in *Tripwire* blog series (2), accessed on 2015/01/04 at http://www.tripwire.com/state-of-security/security-data-protection/developing-cyber-intelligence-analyst-skills/ .

Lee, R.M. (2014c) 'Cyber intelligence collection operations', *Tripwire* blog series (3), accessed on 2015/01/04 at http://www.tripwire.com/state-of-security/security-data-protection/cyber-intelligence-collection-operations/ .

Lee, R.M. (2014d) 'Cyber counterintelligence: From theory to practice', *Tripwire* blog series (4), accessed on 2015/01/04 at http://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/ .

Lee, R.M. (2014*e)* 'Cyber threat intelligence', *Tripwire* blog series (5) accessed on 2015/01/04 at http://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/ .

Lomans, M. (2017), Netherlands Defence Academy, personal correspondence with and feedback to the author.

Lowenthal, M.M. (2012*) Intelligence: From secrets to policy*, 5th Edition, Sage Publishers, California, US.

MacCauvlei Learning Academy. (2016). *Higher certificate in occupational directed education, training and development practices*. Pretoria: unpublished.

Mallett, R, Hagen-Zanker, J, Slater, R & Duvendack, M (2012) 'The benefits and challenges of using systematic reviews in international development research' in the *Journal of Development Effectiveness,* 4(3): 445-455.

Mandiant – FireEye (2015) *M-Trends 2015*, accessed at https://www2.fireeyecom/rs/fireye/images/rpt-m-trends-2015.pdf .

Mattern, T. *et al.* (2014) "Operational levels of cyber intelligence*", International Journal of Intelligence and Counterintelligence*, 27(4):703–719.

Maxwell, J.A. (2012). *Qualitative research design: An interactive approach,* 3rd Edition, Sage, London, UK.

Mena, J. (2003) *Investigative data mining for security and criminal detection*, Butterworths Heinemann, Burlington (Massachusetts), US.

Merriam-Webster online (2017), Search 'cyber', accessed at 03 March 2015 at https://www.merriam-webster.com/dictionary/cyber .

Miler, N.S. (1980) 'What is counterintelligence – Discussants' in Godson, R. (ed*.), Intelligence requirements for the 1980s: Counterintelligence*. National Strategic Information Center, Washington D.C., US.

Miles, M.B. & Huberman, A.M. (1994) *Qualitative data analysis: An expanded source book*, Sage, California, US.

Molander, R.C., Riddle, A.S. and Wilson. P.A. (1996*) New face of war: strategic information warfare*, RAND Institute, Santa Monica, US.

Molander, R.C., Wilson, P.A., Mussington, D.A. & Mesic ,R.F. (1998) *Strategic information warfare rising*, RAND Institute, Santa Monica, US.

Monk, T., van Niekerk, J., & von Solms, R. (2010). 'Sweetening the medicine: educating users about information security by means of game play', *Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists*. Bela Bela, South Africa.

Nakashima, E. (2013) 'To thwart hackers, firms salting there servers with fake data' in *The Washington Post*, accessed on 22/03/2013 at http://articles.washingtonpost.com/2013-01-02/world/36211654_1_ hackers-servers-contract-negotiations

Nolan, J.A. (1997) 'Confusing counterintelligence with security can wreck your afternoon' in *Competitive Intelligence Review*, 8(3):53–61.

Panda Security Labs (2018) *The hunter becomes the hunted: How cyber counterintelligence works*, accessed on 06/11.2018 at https://www.pandasecurity.com/mediacenter/panda-security/cyber-counter intelligence/

Prunckun, H. (2012) *Counterintelligence: Theory and practice*, Rowman & Littlefield Publishers, Plymouth, UK.

Prunckun, H (2014) 'Extending the theoretical structure of intelligence to counterintelligence', *Salus Journal*, vol. 2. no. 2, 31-49.

Prunckun, H (ed.) (2018) 'Weaponization of Computers', *Cyber Weaponry Issues and Implications of Digital Arms*, Springer, Cham, Switzerland.

Putnam, R. T. (2015) *Digital mirrors casting cyber shadows - the confluence of cyber technology, psychology, and counterintelligence*, Master of Science (capstone project), Utica College.

Quiggin, T (2007) *Seeing the invisible – National security in an uncertain age,* World Scientific Publishers, London, UK.

Riley, S. (2015) *Insights to modern threat intelligence*, accessed at https://www.linkedin.com/pulse/insights-modern-cyber-threat-intelligence-shawn-riley?articleId=7011683228767036224 .

Roper, C., Grau, J., & Fischer, L. (2006). *Security education, awareness and training: From theory to practice*, Elsevier Inc, Oxford, UK.

Ruighaver, A.B., Warren, M. & Ahmad, A. (2011) 'Does traditional security risk assessment have a future in information security' in *Journal of Information Warfare*, 10 (3).

Schoeman, A. (2015) 'Demystifying threat intelligence' in *Infosecurity Magazine*, accessed on 13/07/2016 at http://www.infosecurity-magazine.com/opinions/demystifying-threat-intelligence/ .

Shulsky, A.N. & Schmitt, G.S. (2002) *Silent warfare – Understanding the world of intelligence*, 3rd Edition, Potomac Books, Dulles, US.

Sigholm, J. & Bang, M. (2013) 'Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats' in *Proceedings of the European Intelligence and Security Informatics Conference (EISIC)*, *I.E.E.E*, Uppsala, Sweden.

Sims, J.E. (2009) 'Twenty-first-century counterintelligence' in Sims, J.E. & Gerber, B. (eds) *Vaults, mirrors and masks – Rediscovering U.S. counterintelligence,* Georgetown University Press, Washington D.C., US.

Sithole, T.S., Duvenage, P.C., Jaquire, V.J. & von Solms, S. H. (2019) 'Eating the elephant - a structural outline of cyber counterintelligence awareness and training' in *Published Proceedings of the 17th European Conference on Cyber Warfare and Security*, Stellenbosch, South Africa, February.

Schmitt, M. N. (ed.) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, UK.

Smyth, R. (2004) 'Exploring the usefulness of a conceptual framework as a research tool: A researcher's reflections' in *Issues in Educational Research*, 14(2):167–180.

Snow, D.M. (2004) *National security for a new era – Globalization and geopolitics*, Pearson Incorporated, New York, US.

Steele, R.D. (2007) 'Open source intelligence' in Johnson, L.J. (ed.) *Strategic Intelligence – The intelligence cycle* , Volume 2, Praeger Securities, Westport, US.

Stech F.J. & Heckman K.E. (2018) 'Human Nature and Cyber Weaponry: Use of Denial and Deception in Cyber Counterintelligence' in Prunckun, H (ed.) *Cyber Weaponry Issues and Implications of Digital Arms*, Springer, Cham, Switzerland.

Sterling-Folker, J. (ed.) (2006) *Making sense of international relations theory,* Lynne Rienner Publishers, Colorado, US.

Stilianos, V., Llewellyn, E. & Tubb, C. (2007) 'Using deception for assuring security' in *Published Proceedings of the 2nd International Conference on Information Warfare and Security*, Monterey, California, March.

Stone, G.M. & Bluitt K. (1993) 'Future law enforcement and internal security communications architecture employing advanced technologies', *IEEE Publication CH3372-0/93*, pp. 194 -202.

Stone, G.M. & Tucker R.S. 1988, 'Counterintelligence and unified technical security programs', Proceedings of the *IEEE International Carnahan Conference on Security Technology: Crime Countermeasures*, New York, US.

Stroz Friedberg (2017) *2017 Stroz Friedberg Cybersecurity Predictions Report*, accessed on 03/03/2017 at https://www.strozfriedberg.com/wp-content/uploads/2017/01/2017-Stroz-Friedberg-Cybersecurity-Predictions-Report.pdf .

Taylor, S.A. (2007) 'Definitions and theories of counterintelligence' in Johnson, L.K. (ed.), *Strategic intelligence – Counterintelligence and counterterrorism: Defending the nation against hostile forces,* Volume 4, Praeger Securities, Westport, US.

Teti, A (2016) 'Cyber counterintelligence – Il controspionaggio nel cyberspazio' ['Cyber Counterintelligence – counterespionage in cyberspace'] *nosis - Italian Intelligence Magazine*, Information and Internal Security Agency, Vol 4/2016, pp 151 – 158, viewed 30 April 2018 at http://gnosis.aisi.gov.it/ gnosis/Rivista49.nsf/ ServNavig/49-37.pdf/$File/49-37.pdf?OpenElement

Thomason, S. (2013). 'People –the weak link in security', *Global Journal of Computer Science and Technology Network*, Web & Security, 13(11).

Toth, P., & Klein, P. (2013, October). *NIST special publication 800-16 - A role-based model for federal information technology/ cyber security training*. Retrieved 09 September 2018, from http://csrc.nist.gov/publications/PubsDrafts.html#800-16-rev1

Treverton, G.F. *et al* (2006) *Toward a theory of intelligence* – Workshop Report, RAND Cooperation, accessed on 14 February 2008 at http://www.rand.org/pubi/larf/ proceedings /2006/Rand-CF219.pdf .

United States of America (2013) Office of the National Counterintelligence Executive. *Protecting key assets: A corporate counterintelligence guide*, accessed 03 March 2018 at https://www.dni.gov/files/NCSC/documents/Regulations/ProtectingKeyAssets_CorporateCIGuide.

United States of America (2004) Department of Defence, *Dictionary of Military and Associated Terms (12 April 2011 as amended through 7 October 2004)*. Available at http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%2804%29.pdf

United States of America (2001) *DoD Dictionary of military and associated terms,* Department of Defense, Washington DC, US.

United States of America (2013) Department of Homeland Security, *Protecting Key Assets: A Corporate Counterintelligence Guide*, Digital Library, accessed 12 September 2018 at https://www.hsdl.org/?view&did=791221.

United States of America Naval War College (2019) *Library Guidelines* _Counterintelligence_By_Era_CyberThreat, viewed 24 January 2019, <https://usnwc.libguides.com/c.php?g=661096&p=4695517>.

United States of America Naval War College (2018a) *Library Guidelines* _Counterintelligence_By_Era_CyberThreat, viewed 02 August 2018, <https://usnwc.libguides.com/c.php?g=661096&p=4695517>.

United States of America Naval War College (2018b) *About U.S. Naval War*, viewed 02 August 2018, < https://usnwc.edu/About >.

United States of America (1996) *Operations security intelligence threat handbook*, Interagency Operational Security Support Staff, accessed on 11/08/2007 at http:www.fas.org/irp/nsa/ioss/threat96/part03.htm .

University of Johannesburg (2018a) *The Cyber Counterintelligence Project _Centre for Cybersecurity.* <http://adam.uj.ac.za/csi/CyberCounterintelligence. Html>

University of Johannesburg (2018b) *Academic regulations 2018*, Available at https://www.uj.ac.za/about/Documents/Academic-Regulations-2018.pdf

University of Johannesburg (2018c) *Assessor's Feedback Report: Conceptual Framework for Cyber Counterintelligence*, Faculty of Science, 12 March, Johannesburg.

Utica College (2018) *Cybersecurity and Information Assurance Faculty*, viewed 24 August 2018 at https://www.utica.edu/academic/ssm/cybersecurity/faculty.cfm

Van Cleave, M.K. (2007) *Counterintelligence and national strategy*, School for National Security Executive Education, National Defense University Press, Washington D.C., US.

van den Berg, M. A. (2018) *Intelligence practices in South Africa as a hybrid political regime – a meta-theoretical and theoretical analysis,* unpublished PhD thesis, Northwest University, Potchefstroom, South Africa.

Van Derwerken, J., & Ubell, R. (2011). 'Training on the cyber security frontlines' *American Society for Training & Development*, pp 46-50.

van Niekerk, B. & Maharaj, M.S.(2011) 'The Information Warfare Life Cycle Model', *SA Journal of Information Management* 13(1).

van Niekerk, B., Ramluckan, T. & Duvenage, P.C. (2019) 'An analysis of selected cyber intelligence texts' in *Published Proceedings of the 18th European Conference on Cyber Warfare and Security*, Coimbra, Portugal, July.

Venkatesh, V. (2018) Authorship credit: *Thoughts for PhD students and faculty mentors*, viewed 20 August 2019, <https://decisionsciences.org/authorship-credit-thoughts-for-phd-students -and-faculty-mentors/>

VeriSign (2012) *Establishing a formal cyber intelligence capability*, accessed on 22/10/2017 at https://www.verisigninc.com/assets/whitepaper-idefense-cyber-intel.pdf .

von Solms, S. H. (2014) *'Cyber counter-intelligence makes a difference' on ITWeb*, accessed on 11 November 2014 at http://www.itweb.co.za/index.php?option=com_content &view=article&id=134136

Warren, M. (ed.) (2013) *Case Studies in Information Warfare and Security for Researchers, Teachers and Students*, Academic Conferences and Publishing International Limited, Reading, UK.

Wettering, F.L. (2000) 'Counterintelligence: the broken triad' in *International Journal of Intelligence and Counterintelligence*, 13(3): 265-30

ANNEXURES

This section provides peer-reviewed papers and articles published and leading up to the thesis. A quantitative estimation of the candidate's authorship contribution in respect of conceptualisation, ideas, theory, design and writing (Venkatesh 2018) is given as a percentage in square brackets.

ANNEXURE A

2013 International Conference on Adaptive Science and Technology (ICAST 2013)

ICAST 2013

CSIR International Convention Centre Pretoria
25 – 27 November 2013

IEEE Catalogue Number: CFP1392F-POD

ISBN: 978-1-4799-3068-5

The Case for Cyber Counterintelligence

Petrus Duvenage *
State Security Agency
South Africa
*The author contributed to the article in his personal capacity. Views expressed in the article should not be construed as official government views or interpretations.

Sebastiaan von Solms ('Basie')
Director: Centre for Cyber Security
Academy for Computer Science and Software Engineering University of Johannesburg
South Africa

Abstract— A paradigmatic shift in thinking on cyber security in the 21st century is gaining momentum. This turn in thinking is rooted in a widening acknowledgment that conventional cyber security solutions no longer offer adequate protection in the face of threats posed by role players such as nation states, criminal syndicates, corporate spies, terrorists, hacktivists and rogue individuals. It is clear that the securing of cyber space depends not only on raising the bar in respect of existing measures, but also need to involve proactive action focussing on threat agents. Views are, however, not so clear on what such proactive action should entail and how this should be integrated with conventional cyber security measures. Similarly, conceptual clarity is lacking on the configuration of an integrated response attuned to the fast changing threatscape.

The paper firstly examines the cyber threatscape and the challenges this poses. It proceeds with advancing cyber counterintelligence as a conceptual and practicable alternative to coherently and proactively meeting cyber security challenges. Although cyber counterintelligence is not a novel concept, it is academically under-explored with open-source literature on this subject relatively sparse. In particular, the quest for an integrated conceptual model for cyber counterintelligence is still in its infancy. This paper does not purport to offer a refined model, but endeavours to advance a few building contours useful to its construction. Compiled for a wide target audience which includes business professionals and academia, the paper is underpinned by principles and constructs derived from statutory counterintelligence theory and practice.

Keywords— *cyber counterintelligence, cyber espionage, cyber security*

Published in: 2013 International Conference on Adaptive Science and Technology

Date of Conference: 25-27 Nov. 2013

Date Added to IEEE *Xplore*: 09 January 2014

Electronic ISBN: 978-1-4799-3067-8

ISSN Information:

Electronic ISSN: 2326-9448

Print ISSN: 2326-9413

Publisher: IEEE

ANNEXURE B

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Proceedings of the
13th European Conference on Cyber Warfare and Security

The University of Piraeus
Greece
3-4 July 2014

Edited by
Andrew Liaropoulos and George Tsihrintzis

acpi

A conference managed by ACPI, UK

Papers have been double-blind peer reviewed before final submission to the conference. Initially, paper abstracts were read and selected by the conference panel for submission as possible papers for the conference.

Many thanks to the reviewers who helped ensure the quality of the full papers.

These Conference Proceedings have been submitted to Thomson ISI for indexing.

Further copies of this book and previous year's proceedings can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-910309-25-4
E-Book ISSN: 2048-8610
Book version ISBN: 978-1-910309-24-7
Book Version ISSN: 2048-8602
CD Version ISBN: 978-1-910309-26-1
CD Version ISSN: 2048-8629

Published by Academic Conferences and Publishing International Limited
Reading
UK
44-118-972-4148
www.academic-publishing.org

Preface

This year sees the 13th European Conference on Cyber Warfare and Security (ECCWS 2014), which is hosted by The University of Piraeus, Greece.

The Conference Chair is Andrew Liaropoulos, from the University of Piraeus, Piraeus, Greece. The Programme Chair is George Tsihrintzis, University of Piraeus, Piraeus, Greece.

The Conference continues to bring together individuals working in the area of cyberwar and cyber security in order to share knowledge and develop new ideas with their peers. The range of papers presented at the Conference will ensure two days of interesting discussions. The topics covered this year illustrate the depth of the information operations' research area, with the subject matter ranging from the highly technical to the more strategic visions of the use and influence of information.

The opening keynote is given by Prof. Dimitris Gritzalis, Director of the Information Security & Critical Infrastructure Protection (InfoSec) Laboratory, Athens University of Economics and Business, Greece on the topic of "Open-Source Intelligence produced from Social Media: A proactive Cyber Defense tool" and the second day keynote will be presented by Prof. Nikolaos Bourbakis, IEEE Fellow, Director of the Assistive Technologies Research Center (ATRC) Wright State University, USA, on the topic of "Cyber-Security Challenges in the Cyber-Space".

With an initial submission of 71 abstracts, after the double blind, peer review process there are 27 Research papers, 7 PHD Research papers, 2 Masters Research papers, 1 Non Academic paper and 1 Work in Progress Paper published in these Conference Proceedings. These papers come from all parts of the globe including Australia, Austria, Czech Republic, Finland, Greece, Lithuania, New Zealand, Nigeria, Norway, Portugal, Republic of South Africa, Turkey, UK and USA.

I wish you a most interesting conference and an enjoyable stay in Greece.

Andrew Liaropoulos and George Tsihrintzis,
University of Piraeus, Greece

June 2014

Putting Counterintelligence in Cyber Counterintelligence

Petrus Duvenage[1] and Sebastian von Solms[2]
[1] Centre for Cyber Security, University of Johannesburg, South Africa
[2] Centre for Cyber Security, University of Johannesburg, South Africa
duvenage@live.co.za
basievs@uj.ac.za

Abstract: Businesses and governments alike are grappling with configuring their cyber security postures effectively in a manner to account for rapid changes in the cyber threatscape. Defensively security policies and measures (inclusive of software and hardware technologies) on their own are wholly inadequate in protecting against proliferating threats. An effective approach for securing and advancing cyber interests will have to combine more proactive defences with intelligence on, and the engagement of, adversaries. Offensive and defensive measures, in turn, should be integrated with an institution's strategy and objectives. Appropriately conceptualised, Cyber Counterintelligence (CCI) could meet these requirements and offer a practicable approach for governments, businesses and other sizable entities. There is a precondition. To be effective, CCI should be an integral part of multi-disciplinary Counterintelligence (CI) – conceptually and in practice. However, at least in as far as consulted academic literature is concerned, such conceptualisation is lacking. Disconcertingly, the theoretical discourse about CCI could be gaining momentum without a categorical explication of CI. This paper conceptualises CCI as part of CI. To this end a cursory primer on CI is provided. Building on this primer, the paper proceeds with advancing:

(i) A definition of CCI.
(ii) A three-tiered postulation for conceptually integrating CCI with multi-disciplinary CI, Intelligence and Strategy.
(iii) A taxonomy of CCI tools, methods and means.
(iv) A matrix that has the dual purpose of (a) categorising CCI tools, methods and means; and (b) plotting a CCI posture in accordance with the nature and the needs of a specific institution.

Keywords: counterintelligence, cyber security, cyber counterintelligence.

1. Introduction

What was seen as a paradigmatic shift in thinking at the turn of this decade is now commonly accepted – conventional cyber security we have been relying on is deteriorating on all fronts (Lües 2012). As a result, cyber space is now probably more insecure than it has ever been (Bodmer et al 2012). It is also likely to be the most secure than it is going to be for the foreseeable future. It is, simply put, going to get much worse. In this regard, the World Economic Forum's (WEF) 2104 Global Risk Report warned of "digital disintegration" when it stated: "The world may be only one disruptive technology away from attackers gaining a runaway advantage, meaning the Internet would cease to be a trusted medium for communication or commerce" (WEF 2014). The report continues with identifying the foremost "technological risks" for the immediate future as the breakdown of critical informational infrastructure and networks, an escalation of large scale cyber-attacks and incidents of data fraud an unprecedented scale (WEF 2014). Even early on in 2014, these are no longer risks but manifesting trends. Attesting to this is the continuing prominence in mass-media media reporting on the escalating detrimental impact of cyber criminals, hacktivists and other role-players. Simultaneously the pervasiveness of nation states' cyber surveillance by the intelligence apparatuses of not only the United States (U.S.) and United Kingdom (UK), but also the People's Republic of China (PRC) and Russia continue to make headlines.

With the awareness of conventional cyber security's faltering, both state and non-state actors have been intensifying the quest for ways to more effectively protect and advance their cyber interests and, in the case of service providers and vendors, those of their clients. As could be expected, solutions offered in the market place vary considerably. Buzzwords and marketing slogans currently gaining favour include counter exploitation, threat intelligence, offensive measures, hacking back, threatscape and intelligence software analytics (IBM 2013, Helton 2013). Common to most of these solutions advocated, is recognition of the imperative of intelligence on threats actors and the need to engage threats pro-actively/offensively. There is a sense of taking the fight to adversaries. The use of such notions and phrases would have been encouraging if it

was indicative of more organisations "moving towards intelligence-driven risk management and decision-making models." (Helton 2013). As it currently stands the use of these terms is, however, disturbing for three inter-related reasons. Firstly, the terms are used vaguely and without the proper context from the statutory intelligence practice from which they are often derived. In marketing jargon 'intelligence' is used interchangeably with 'data and information.' Consequently, solutions offered under the rubrics of 'intelligence' may not solve the problems for which they purport to be the fix. In a similar vein the opting for quick-fix offensive actions, not dovetailed with an appropriately configured defensive posture, is inviting disaster. Equally disconcerting, solutions and terms are sometimes thrown around without due and categorical stipulations that some aspects of cyber defence and offense are the exclusive prerogative of the state apparatus in most countries. These functions ought not to be 'out-sourced' to other entities. Secondly, solutions being offered are essentially technical and tactical in nature. As important as they are, technical and tactical measures on their own, were mentioned earlier, as being insufficient to confront the sophisticated threat actors about whom we are most concerned. Social engineering, to cite one example, "played a part in nearly every major hack or breach in 2013 yet it still stays in the background when we consider security controls. This is something that needs to change as we move forward." (ISC^2 2013). Thirdly, these solutions are presented as neat 'add-ons' or 'plugins' to be used as a layer additional to existing cyber security measures. 'Add-ons' seldom have, and certainly will, not in future, offer adequate protection against advanced adversaries. For sizable institutions with significant digital and information interests to face up to such adversaries, cyber security needs to be coherently part of their DNA and not mere feel-good plasters offering little real protection.

There is a way in which such synergy can be achieved and the tables turned on cyber adversaries. This paper posits cyber counterintelligence (CCI) as a practicable approach to effectively securing and advancing cyber interests. From this perspective, malicious cyber actions are not all bad news. The good news is that we can exploit malicious cyber actions to our advantage and the detriment of the adversarial instigators. There is, however, a precondition and there are no half measures. To be effective CCI needs to be properly conceptualised and implemented. If not, it is your highway to hell that could end in self-destruction. For a substantial part, this conceptualisation entails the application of time-tested counterintelligence (CI) notions to the cyber sphere. It is a case of going back to counterintelligence fundamentals in order to enable our prosperity in the cyber sphere today and in the future. It is thus a case, as suggested by the paper's title, of going back in order to successfully move to a more secure cyber future.

This paper's primary aim is to provide a conceptual baseline that could aid in stimulating the academic discourse on CCI. Consequently, it ensues with a cursory overview of the status of CCI in the public and academic discourse on cyber security. An academic self-awareness of CCI under-theorised status is after all a first step in addressing this near void. The paper proceeds with advancing CI and CCI constructs hopefully useful to this discourse. Rather than aiming to impart radically new concepts, the emphasis is on presenting existing knowledge in a manner conducive to further academic debate. Such conceptual 'building blocks' include a definition and delineation of the CI as a CCI sub-discipline, a taxonomy for CCI methods and means as well as a CCI matrix for configuring an offensive-defensive posture. It concludes with some views on CCI's future and by suggesting areas for further academic enquiry.

As noted above, the following section reflects on CCI under-theorised status, since such awareness is an important first step in make progress with the academic discourse.

2. Cyber Counterintelligence's Under-Theorised Status

In one form or the other cyber counterintelligence has been practised as part of the statutory counterintelligence functions in various intelligence communities for well over two decades. CCI has also been offered as service by a few niche companies for well over a decade. Until very recently, however, CCI has not really gained traction outside the statutory security structures and the small batch of clients the niche companies served. Despite the key it holds to secure cyber interests for state and non-state actors, CCI entered the second decade of the 21st century underappreciated and underexplored in policies and other literature in the public domain. The overwhelming majority of governments' cyber security policies do not make any references to counterintelligence. In the few instances that the concept is cited, counterintelligence is hardly at the centre. (Remark: A notable exception in this regard is the U.S.' Comprehensive *National Cyber Security Initiative* that assigns a central role to with counterintelligence.

Anecdotal indications are that CCI has fast been gaining traction during the last two years. The 2013 proceedings of the 12th European on Cyber Warfare and Security (ECCWS), for example, comprise of 44 papers and is a voluminous 406 pages in length (Kuusisto & Kurkinen, 2013). Not one of these papers makes mention of CCI. There is in fact only one sentence in the whole of the proceedings that makes cursory reference to the concept counterintelligence generally (Kuusisto & Kurkinen, 2013: 244). One year on and ECCWS 2014 features a dedicated mini-track to Cyber Intelligence/ Counterintelligence. While this certainly reflects an increased awareness of CCI, contributions are scarce. As far as could be surmised from the listing of abstract titles, this was the only paper to be presented at ECCWS 2014 that has CCI as focus or counterintelligence in its title.

While a few commendable books have been published on the subject, these are minuscule in comparison with the proliferating material on cyber security generally. The shift in emphasis towards CCI is nonetheless also apparent here. An outstanding work by Bodmer *et al* was first published in 2012 with the title *Reverse Deception – Organized Cyber Threat Counter- Exploitation* (Bodmer et al 2012). The edition due for release in 2014 – which as far as could be surmised from pre-launch advertising retained the core of the 2012 edition – is more aptly entitled *Hacking Back: Offensive Cyber Counterintelligence* (Bodmer et al 2014).

Although CCI is set to gain in prominence, the participation in and agenda of this discourse will inevitably be influenced by the relative obscurity of CI in general. CCI will be demonstrated in further sections as a sub-set of the broader, multi-faceted CI discipline. It thus follows that contributions to CCI would need to be preceded by some grounding in CI. CI, however, and herein lies the glitch, is in itself academically obscure and underappreciated. This obscurity is as old as its inception as a formalised discipline in the run-up to the Second World War. Some would argue that this can be ascribed to the fact that a large part of CI work relies for its effectiveness on secrecy. Yet, as we are reminded by Meyer (1987), we do not need to reveal secrets to talk seriously about matters of Intelligence. A more likely reason for CI's obscurity in the academic debate is to be found in the fact that it is arguably the most complex and least understood of all Intelligence disciplines (Godson 2001). The following statement by a U.S. CI veteran in the midst of the Cold War has lost none of its relevance: "It is not easy, nor can one feel confident, to re-enter this world where, it has been said, the tortuous logic of counterintelligence prevails ... Unfortunately, there seems to be no easy way to explain counterintelligence ... Because effective counterintelligence is a combination of so many aspects." (Miller, 1980) Even among policy makers, scholars and "national security practitioners" in foremost intelligence communities such as those of the U.S., "the role of counterintelligence remains little known or understood" up to this day (Van Cleave 2007).

Since the role, functions and importance of CI is opaque within statutory intelligence circles, the reluctance of 'techies' to apply this concept to the cyber sphere is understandable. In a similar vein, those skilled and experienced in more conventional counterintelligence do not necessarily have a sound working knowledge of technical cyber. If we are not clear on a conceptual level, we can hardly make progress in the academic discourse, thereby eventually affecting our ability to implement sound solutions. In the conceptual difficulties of CI also lies the opportunity. If we can understand and explain CI, we can explain CCI and unlock the latter's potential as force multiplier.

This section illustrated the need for contributions to the budding field CCI to be clearly rooted in CI. In line with this contention, the next section provides a conceptual primer of CI.

3. A Primer on Counterintelligence

Counterintelligence has been practised and described for millennia. Some enduring principles were penned in 500 B.C. by the much-quoted Sun Tzu in a specific chapter in his *The Art of War* devoted to the use of spies and counter-spies (Giles 2002). The term in its contemporary connotations entered the English lexicon in the mid-1930's (Dictionary.com 2013). For some, counterintelligence is all about spies outgunning adversarial spies. For others, it invokes mundane security measures such as computer passwords, restrictions on the use of computing equipment, security guards, access control and the like. Counterintelligence is both of these aspects and so much more (Duvenage & von Solms 2013).

3.1 Delineating counterintelligence

Counterintelligence can be defined as the collective of measures undertaken to identify, deter, exploit, degrade, neutralise and protect against adversarial intelligence activities deemed as detrimental or potentially detrimental to the own interests (Duvenage 2010). The term 'counterintelligence' is thus an abbreviated form for the countering of hostile intelligence activities. Adversaries engaging in hostile intelligence actions include nation states, corporate entities, criminals, activists, individuals and any combination of these.

Adversarial intelligence activities include espionage, deception (disinformation), influencing and some other forms of covert action that can have disruptive and destructive outfalls. Of these different intelligence activities, espionage is the most central. Espionage to obtain protected information in order to gain a competitive advantage can be an end in itself; or such information can be used to further other malicious ends such as data manipulation, disinformation and disruption. Sophisticated adversaries execute their intelligence actions through the exploitation of humans (HUMINT) and technical means (TECHINT). The latter, in turn, comprise Signal Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT) and Cyber Intelligence (CYBINT). These conduits and their relation to adversarial intelligence ends can graphically be depicted as follow:

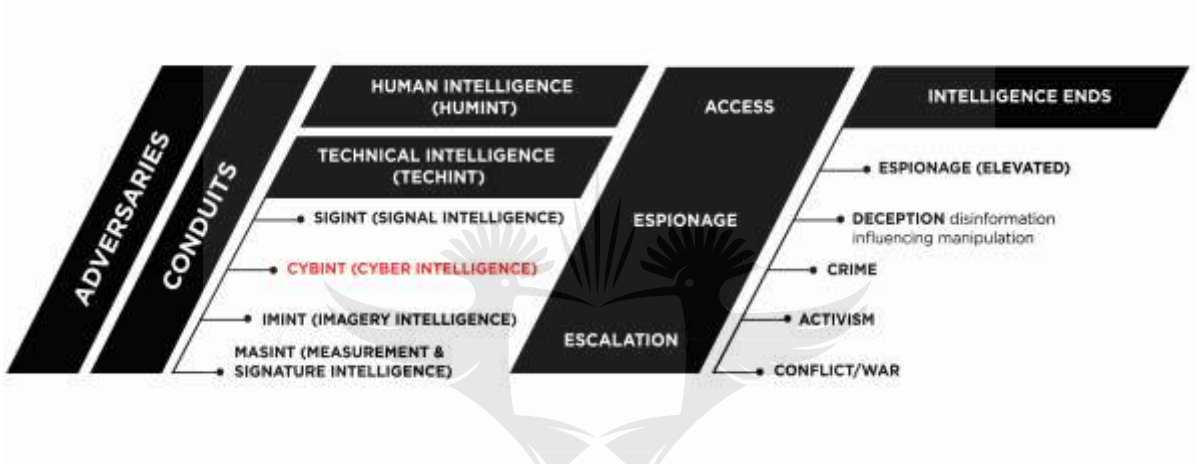


Figure 1 Adversarial Intelligence: Conduits and Ends

Several revelations by the whistle-blower Edward Snowden provide a practical illustration of the above. During September 2013, for example, *The Guardian* newspaper revealed that the British and U.S. Agencies run HUMINT operations to "help secure an insider advantage" (Ball et al 2013). To this end the British Government Communications Headquarters (GCHQ) established a HUMINT Operations Team (HOT) "responsible for identifying, recruiting and running covert agents in the global telecommunications industry." (Ball et al 2013). These operations enabled the Agency to "tackle some of its most challenging targets" specifically in as far as the breaking of encryption was concerned (Ball et al 2013). In this instance success in the field of CYBINT thus depended on the effectiveness of HUMINT operations. The reverse is of course also true. Given the high and growing digital dependence, CYBINT is often a critical enabler in the HUMINT sphere. To be effective CI needs to counter all types of adversarial intelligence activities and, in the case of high-end adversaries, it has to do so in more than one or all of the conduits.

3.2 Counterintelligence: Measures, Means and Modes

In order to execute its mission CI relies on measures and means that vary from the passive-defensive to active-offensive. At the one end of the spectrum, passive-defensive measures strive to deny adversaries access to protected information assets. They aim to reduce vulnerabilities through a combination of policies, procedures and practices – sometimes referred to on a lighter note as "gates, guards, guns, and dogs."(Francq 2001). Apart from denying opponents access, properly instituted passive-defences measures are like caste walls. In addition to preventing common intrusions, their presence discourages intrusion attempts and consequently serves a deterrence function. Examples of passive-defensive measures are access and movement control, perimeter security, alarm systems, safes and vaults, fire prevention measures, key control and the control of the removal and transfer of information from facilities where valued information is located. At the other ends of the spectrum, offensive counterintelligence aims to neutralise a competitor's intelligence efforts through

measures ranging from deception and manipulation to the neutralisation of adversarial intelligence activities and systems. Deception takes various forms and can be achieved through numerous means. Skilfully executed, deception attains a primary counterintelligence aim, which is the manipulation and control of an adversary. This is aptly encapsulated by Codevilla when he states: "Action against the enemy through the enemy's own intelligence is the very consummation of CI." There are of course also aggressive CI measures that overlap with CI's sister-Intelligence discipline covert action. Under certain conditions, assassinations and even extra-ordinary rendition can be classified as active-offensive CI neutralisation measures (Duvenage 2010).

Between passive-defensive and active-offensive lies a wide array of other measures such as pre-employment personnel security; in-service personnel security; technical surveillance countermeasures (TSCM); encryption; surveillance (physical, static, mobile and electronic); double agents; agents and continued monitoring. In most instances, these measures can serve defensive or/and offensive purposes. Defensive counterintelligence tactics and strategies provide information to, and act as triggers to alert the offensive side of the practice. Similarly, offensive operations (for example a source reporting on an adversary's intentions and capabilities) inform the pro-active configuration of defences. It will also be noted that several of these are highly useful in the collection of information on internal vulnerabilities (e.g. organisational weakness and the insider threat), the external environment as well as actual and potential adversaries. It goes without saying that without such information being analysed CI would be blind and unable to execute the defensive-offensive interplay. The following matrix, depicted in Figure 2, is somewhat of an over-simplification but nonetheless useful in conveying the nuanced nature of the offensive-defensive interplay as well as the importance of collection:

DEFENSIVE MODE **Denies adversaries access to and generates information about adversaries**	
Passive Defence Denies the adversary access to information through physical security measures and security systems.	**Active Defence** The active collection of information on the adversary to determine its sponsor, modus operandi, network and targets. Methods include physical and electronic surveillance, dangles, double agents, moles and electronic tapping.
OFFENSIVE MODE **Aims to manipulate, degrade, control and neutralise adversaries**	
Passive Offensive Reveals to the adversary what you want them to see. This could range from selective exposure of actual information to decoys and dummies. The adversary is thus left to draw own inferences and interpretations.	**Active Offensive** The adversary is fed with disinformation and its interpretation thereof manipulated. Disinformation can be channelled through for example double agents and 'moles'. Active-offensive CI could include some forms of covert action. Covert action, in its use here, denotes the targeting of an adversary through the influencing of events, conditions, individuals, groups or institutions to the benefit of a sponsor in a manner not attributable to the sponsor or offering plausible deniability. Influencing is achieved through measures that vary from paramilitary and political actions to propaganda and intelligence assistance.

Figure 2: A Four-Sector Counterintelligence Matrix (Compiled by the authors on the basis of narratives in Sims 2009, Odom 2003 and Godson 2001)

3.3 Counterintelligence Process

The preceding matrix and discussion above, demonstrate CI as intricate and exhaustive discipline. It is not only about defences, but also the concrete advancement of own interest vis-à-vis adversaries. It could be surmised from the above, no matter how well-resourced, the CI endeavour cannot protect all assets and advance all interests all the time. The bodies of information that justify CI protection as well as the systems, processes, institutions and individuals in which such information resides must be identified and prioritised (Prunckun, 2012). Since offensive action carries even higher risks and costs, CI should be crystal clear on it role in this regard. Such clarity in turn presupposes CI to be in synergy with Intelligence and at the centre of a government's or business' strategy. These are the critical roots of the CI premise.

While few would dispute CI's premise, opinions are divided on the structuring of the CI process. This paper favours a process model that differs fundamentally from the traditional (positive) intelligence cycle and

Clarke's target-centric process (Clarke 2004). This process model comprises the following steps (Duvenage & Hough 2011, Duvenage 2013):

1. Identify own information and assets that warrant the expending of counterintelligence resources.
2. Assess own vulnerabilities that increase the risk of information being compromised.
3. Scan the environment and identify actual or potential threat-agents.
4. Collect information on threat-agents and appraise the risks.
5. Re-assess own vulnerabilities and review defences.
6. Develop sets of counterintelligence measures and projects (offensive and defensive).
7. Implement the recommended countermeasures and projects.
8. Continually assess and adapt the implemented countermeasures to compute the changing environment.

The apparent simplicity of this model in certain respects masks some intricacies of the counterintelligence process. In the case of offensive counterintelligence, for example, espionage adversaries will be engaged through a pattern of activities interwoven with the broader counterintelligence processes. Offensive counterintelligence, in other words, will be performed as a sub-process of step 6 outlined above. This sub-process draws an important distinction between an 'espionage adversary' and an 'espionage target'. An 'espionage adversary' is the ultimate sponsor of an intelligence effort, while the counterespionage target is the instrumentality with which intelligence activities are conducted. This instrumentality is targeted by an opposing entities counterespionage structure – hence the phrasing 'counterespionage target'. A nation state and its intelligence service would, for example, be espionage adversaries and the proxies for conducting the actual espionage, the counterespionage targets. Such proxies could be recruited agents or third entities (for example front companies). Employing this distinction, the offensive counterespionage process – which is executed per step 6 of the process model above - will typically have the following sub-steps (Duvenage & Hough 2011):

6.1 Identification of espionage adversaries.
6.2 Prioritisation of espionage adversaries.
6.3 Investigation of espionage adversaries.
6.4 The engagement of counterespionage targets.
6.5 Exploitation of counterespionage targets.
6.6 Neutralisation of targets and termination of operation

This section provided a primer that demarcated CI, explained CI measures and modes and offered propositions on the CI process. Building on this overview of CI, the paper proceeds with conceptualising CCI.

4. Conceptualising Cyber Counterintelligence

This section provides a provisional definition of CCI, advances a model for integrating CCI with CI and Intelligence and outlines some CCI methods, means and modes.

4.1 Defining and Delineating Cyber Counterintelligence

While various definitions for CCI have been advanced, none of these specifically explicate the relationship between CCI and CI (cf. Carrol 2009, Bodmer et al 2012, Farchi 2012). In keeping with the paper's central contention, CCI is defined as that subset of multi-disciplinary CI aimed at deterring, preventing, degrading, exploiting and neutralisation adversarial attempts to collect, alter or in any other way breach the C-I-A of valued information assets through cyber means. Expanding on this definition, it is postulated that CI delineates CCI on the following three tiers (Duvenage & von Solms 2013):

- Applied to the cyber context, CI theory and practice provides a conceptual template for modelling CCI actions in the safeguarding and advancing of cyber interests. Mirroring CI, CCI has offensive and defensive missions that are distinguishable but not separable.
- To be effective, cyber counterintelligence needs to be interlocked with all-field counterintelligence – defensively and offensively. In this sense, CI cements an integrated approach to securing the cyber space. CCI is thus about both the modelling of cyber actions on CI, and the integration of these offensive and defensive actions with conventional CI.
- Effective CI protects and promotes the Intelligence endeavour and business strategy. Since CCI is part of CI, it is also integrated in business strategy and Intelligence.

Figure 3 depicts this three-tiered relationship graphically.

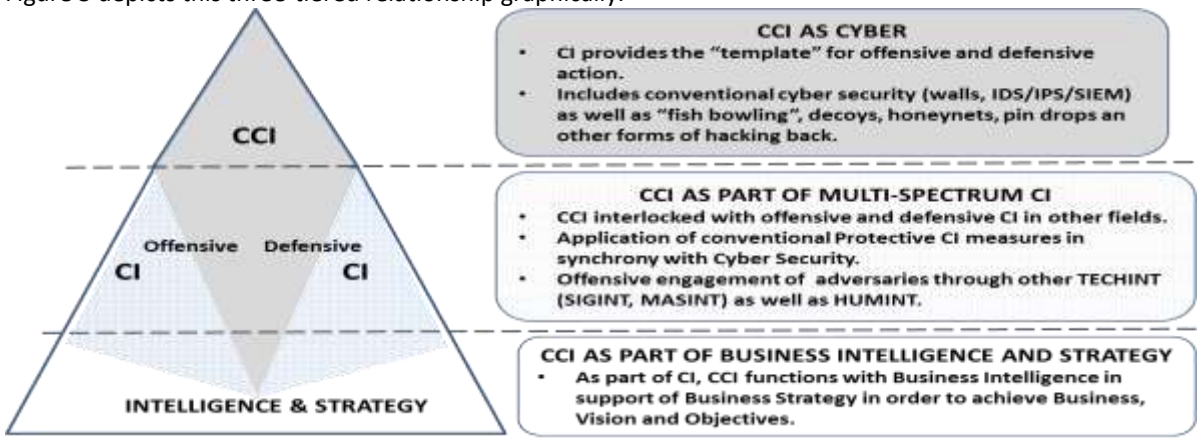


Figure 3: The Cyber Counterintelligence Pyramid (created by the authors)

The postulation, per the narrative and Figure 3, is admittedly cursory and does not purport to conform to the criteria of a conceptual model. However, it could provide a useful premise for further research and the development of a conceptual model for implementation in the cyber domain.

4.2 Overview of Cyber Counterintelligence Methods, Means and Modes

The section above made graphic and narrative reference to defensive and offensive CCI actions. Mirroring CI in general, CCI methods and means can be deployed in offensive and defensive modes, but defy categorisation in watertight compartments. At the very ends of this spectrum there are a few methods and means that could be designated clearly as active-offensive (notably cyber weapons with destructive purpose such as Stuxnet) or passive-defensive (e.g. access control and validation directives). In the main, however, offense-defensive and active-passive are not neat compartments, but rather the manner in, and end towards which, methods and means are deployed (Duvenage & von Solms 2013). This is illustrated in the following matrix, in Figure 4, which depicts the four cyber-counterintelligence modes (postures) an entity could assume:

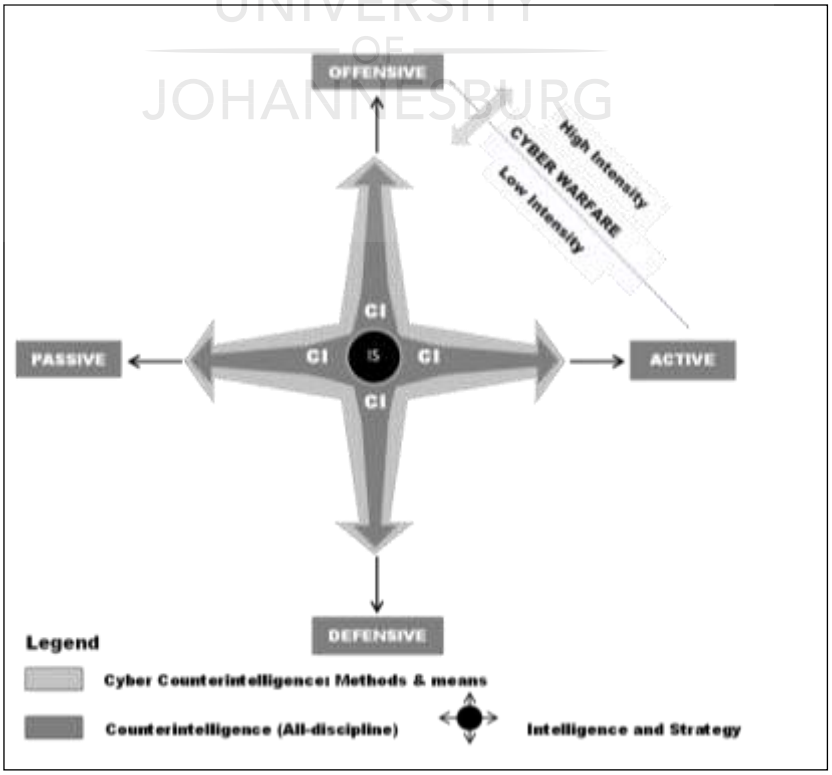


Figure 4: Cyber Counterintelligence Matrix (created by the authors)

The CCI matrix per Figure 4 is more than a notional construct and can be applied practically by entities (with sizable cyber interest and assets) in the plotting of CCI methods and means. The matrix ensures that a presence is maintained, or at the very least that contingency planning is done in respect of all four quadrants. It furthermore facilitates innovation and creativity in the application of methods and means – within legislative parameters of course. Contrary to a misconception, for example, an Intrusion Prevention System can be configured with surprising positive results in executing aims in the other three quadrants. Consequently, the construction of a tabulated taxonomy of CCI methods and means could very well be an oversimplification. Even more so should the taxonomy endeavour to point to parallels that exist between CCI measures and those in CI generally. Nonetheless, at this early stage of conceptualising CCI such a simplification serves as a soundboard for further debate. With this caveat, a cursory taxonomy of CCI methods and means is provided in Table 1:

Table 1: Taxonomy of Cyber Counterintelligence Methods and Means (Adopted from Duvenage & von Solms, 2013)

<table>
<tr><th colspan="3">Defensive Mode</th></tr>
<tr><td colspan="3">Passive ⟶ Active</td></tr>
<tr><td>Deny</td><td>Detect</td><td>Collect</td></tr>
<tr><td>Physical Defensive</td><td>Personnel/User Defensive</td><td>System Defensive</td></tr>
<tr><td>Protects against:
• Unauthorised access to facilities and systems.
• In loco theft of data, hardware.
• Introduction of malware through physical access to systems.
• Physical destruction.
• Unauthorised reading (acoustic, visual, analogue, signals).
• While not conventionally seen as a Physical Defence, supply-chain management has a physical defensive function. It is also part of System Defences.

<u>Remark</u>: Within the area of Physical Security, there is an extensive and strong convergence between CCI and conventional CI. In keep with the article's central contention that CCI ought be seamlessly integrated with CI, the sub-category 'Physical Defensive' is included in this taxonomy. Note is taken of the fact that with other classification criteria some of the measures listed above may excluded from CCI per se.</td><td>Consists of aspects such as
• IT and user personnel vetting, re-vetting and confidentiality agreements.
• Personnel security measures, BYOD user parameters or exclusions.
• User programmes in cyber security which cover policy and procedures for the handling of security incidents and malfunctions.
• Overlapping with system defences, the use of software decoys to mitigate the insider threat.
• Investigations focused on cyber security incidents involving personnel. Could also include digital forensic investigations.</td><td>Comprises a combination of
• Hardware and software such as
✓ Network perimeter-based security (filters, certain firewalls, etc).
✓ Malware scanners.
✓ Integrated automated systems/tools (that collect and evaluate information about devices connected to a network, activities thereon – inclusive of intrusions). Examples of such tools, discussed further on in the table, are decoys and honeynets.
✓ Overlapping with the latter, are IDS and IPS. Depending on its configuration, a honeynet can be defensive or offensive in type/mode. The term fish bowling denotes the defensive configuration. (Remark: See http://ids.cs.columbia.edu/content/ publications. html for extensive work that has been done on IDS/IPS).
• Processes (such as supply- chain management, product verification and testing) are also in part system defences.
• Vulnerability assessments and penetration testing.
• Incident investigation and response. A CERT is per definition defensive – although it might contain offensive elements in its responsive action.
• BYOD regulation in as far as network interfacing is concerned (Also part of Personnel Defenses).</td></tr>
<tr><td></td><td colspan="2">• The use of honeynets and software decoys to mitigate the insider threat is an overlap between personnel and system defensive measures. They are mostly active CCI means.</td></tr>
</table>

<table>
<tr><td></td><td>• Investigations focused on internal cyber security incidents involving personnel. May include digital forensic investigations.</td><td>• Investigations of external cyber intrusions could be part passive and part active system defence.</td></tr>
<tr><td colspan="3">Offensive Mode</td></tr>
<tr><td colspan="3">Passive ⟶ Active</td></tr>
<tr><td colspan="2">Collect Disrupt</td><td>Exploit</td><td>Destroy</td></tr>
<tr><td colspan="2">• Collection of information on and the monitoring of the cyber sphere to detect cyber adversaries and their exploitation of the cyber sphere in a manner that is not own-network restricted (i.e. requires more than deployment of systems described under defensive mode). Could, depending on configuration also include IDS/IPS, honey-client applications (as opposed to host-based honeypots) and data mining.
• The recruitment and handling of virtual agents on underground forums (under true or false flag) that can serve the purpose of collection and/or exploitation. (Under certain circumstances virtual agents can also develop into HUMINT assets).</td><td>Measures taken to exploit and neutralise adversaries activities in the cyber sphere:
• System and honeynet configured offensively with the aim of exploiting and deceiving adversaries. False information is displayed to adversarial reconnaissance tools, network scanners and listeners, etc. This has as one of its aims to lead adversaries in the direction of your own preference.
• Utilisation of virtual agents for offensive purposes.</td><td rowspan="2">Cyber warfare, in the full extent of the term, is typically excluded from the mandate of civilian intelligence communities. A cyber warfare capability should be flexible and allow utilisation without, or in conjunction with, kinetic war.

Nevertheless, a top class civilian CCI outfit will need to have the authority and capacity to very selectively conduct operations that have cyber warfare characteristics. Such cyber CCI operations will share characteristics with covert action. (Covert action aims to influence role-players, conditions and events without revealing the sponsors identity.)

Within business, the use of offensive measures will be determined by the legislative and regulatory framework within which the entity operates.</td></tr>
<tr><td colspan="2">• Cyberespionage on adversaries. Distinguishable from own-system collection (IPS, IDS, honeynets) on the basis that adversarial networks are actively targeted and exploited in accordance with strategic and operational objectives.</td></tr>
</table>

Self-evidently, Table 1 samples only some of the wide array of CCI methods and means. Moreover, and given the length constraints of an article, on a very few of these are further elaborated upon, namely honeypots and decoys, cyber profiling and cyber-agent operations.

It would have noticed that of the means cited above, honeynets feature prominently in the active, passive as well as the defensive and offensive modes. Honeynets have been in use for more than two decades with the principle objective to detect, monitor and gain intelligence on adversarial intrusion on a network (Bodmer et al 2012). In recent years, the purposes of honeynets diversified from its original mostly defensive use to include also a much more active and/or offensive role. Concurrently, the different types of honeypots and configurations thereof continue are sharply increasing. In as far as architecture goes, and depending on specific needs and situations, honeynets can be centralised, distributed, federated, and confederated (Bodmer et al 2012). The diversifying aims of honeynets now include one or a combination of deception, disinformation and the draining of adversarial resources through labyrinths and "rabbit holes" (Nakashima 2013, Duvenage & von Solms 2013). In a similar vein, decoys are highly useful in disrupting external intrusion and/or mitigating the insider threat (Voris et al 2013). The more resourced and sophisticated the adversary, the greater the imperative to attune the staging of honeynets and the content filling of honeypots, honeyfiles and honeytokens in accordance with the opposition's interests and modus operandi (Duvenage & von Solms 2013).

Counter-action with matching sophistication, in turn, requires sound analysis of high-grade information on the environment and adversaries. Unsurprisingly cyber profiling which involves the application of criminal and intelligence profiling methods to the cyber realm is fast gaining field as a CCI specialisation area (Bodmer et al 2012). In order to procure information on actual and potential adversaries, as well as to keep to tabs on hacking communities of all sorts, CCI outfits maintain a layered presence on nets and forums. This presence varies from the deployment of soft and hardware instrumentalities to the cyber equivalent of HUMINT

counterespionage, namely the recruiting, turning and handling witting/unwitting agents (Duvenage & von Solms 2013).

4.3 Cyber Counterintelligence as a multi-disciplinary subset of Counterintelligence

In line with the theoretical outline of the relationship between CCI and CCI (Figure 3 and Figure 4), the practical safeguarding and advancement of cyber interests is a multi-disciplinary endeavour. CCI is thus not only multidisciplinary in itself but is overlaid upon multi-disciplinary counterintelligence. This multi-disciplinary mind set is especially relevant in the face of sophisticated threats. As part of the Edward Snowden revelations it was, for example, reported that the USA and UK Intelligence communities rely on the recruitment and running of HUMINT sources networks in the global telecommunications industry to "tackle" some of their "most challenging targets" - inter alia in the cryptology field (Ball et al 2013). In keep with such multi-dimensional threats, a CI operation in the cyber field could entail a multi-disciplinary team comprising cyber security specialists, strategic analysts, tactical and technical analysts, HUMINT specialists (e.g. agent handlers and intelligence psychologists), cyber-defense technical experts, language experts, ethical hackers, sociologists and religious experts (Bardin 2011). While a sharp edge on the offense, humans are also the weakest and possibly the most ruinous chink in the defensive armour. Powell et al (2013) asserts "an organizations insiders" as "primary threats to cybersecurity … [which are] ….the most difficult to mitigate." Complementary to technical defences, CI personnel fidelity measures and HUMINT counterespionage practices are thus critical. This is being highlighted by unfolding detail around the Edward Snowdon incident.

The convergence of cyber and HUMINT counterintelligence was furthermore demonstrated by a recent re-evaluation of the Aurora attacks. This re-evaluation suggests the Aurora attacks were not, as was initially thought, a People Republic of China (PRC) operation targeting human-rights activists. It was in fact a Chinese counterintelligence operation to determine whether PRC intelligence operations and agents have been compromised to USA intelligence (Corbin 2013). Duvenage & von Solms (2013) cites as a further example of "an integrated CI initiative, a disinformation campaign as part of which the staging and content filling of a honeynet is harmonised with disinformation fed to an adversary through a HUMINT asset (e.g. double agent)."

4.4 Cyber Counterintelligence and Counterintelligence – an integral part of Intelligence and Strategy

CCI, to re-state the paper's recurring theme, forms part of and is guided by the integrated CI endeavour. Consequently, CCI follows the CI processes discussed in Section 3.3. The CI processes, in turn, ought to function in synergy with Positive Intelligence. CI not only safeguards Intelligence operations, but renders inside information on competitors highly useful to executives. In addition; deception, disinformation and other such projects support a company in achieving its business objectives. This is thus a more a practical illustration of the theoretical postulations per Figures 3 and 4 which put business objectives and strategy as the pivot around which CI and CCI evolves.

5. Conclusion

This paper forms part of still spare yet fast growing body of academic literature which views CCI as a practicable approach for governments, businesses and other sizable entities for securing and advancing cyber interests. Proliferating threats and trends affecting cyber security are not all bad news. Contradictory as it may appear, the more extensive adversarial cyber action the greater the potential opportunity could be for counter-exploitation. The call for cyber CCI should not be misconstrued as a call for a free-for-all cyber Wild West. Performed haphazardly and in a silo, CCI is could be self-destructive.

There are several pre-conditions for effective CCI. To be effective, CCI should be an integral part of multi-disciplinary CI – conceptually and in practice. In consulted academic literature, however, such conceptualisation is lacking. For the most part they endeavour to progress with CCI theory construction, without a sound foundational explication of CI. Theory so formulated and models so constructed could hold serious negative repercussions on a practical level. Within counterintelligence, the price for bad theory is eventually costly failures. As pointed out in an earlier contribution: "Conceptual models are not mere theoretical, academic constructs. Models condition our thinking and our approach to practice. What we therefore need is a sound overarching CCI model that can synergistically bind developing theory." (Duvenage & von Solms 2013)

Therefore, this paper firstly aimed to put the counterintelligence in cyber counterintelligence. This was done through conceptualising CCI as part of multi-disciplinary CI and the applications of time-tested CI constructs to the cyber sphere. Secondly, the article offered a few conceptual constructs as contours towards the construction of such a model. So doing, it demonstrated the degree to which conventional, time-tested CI constructs can guide CCI's conceptualisation. The actual construction of a credible model, however, will require extensive in-depth, multi-disciplinary research and debate.

References

Ball, J. et al. (2013) "Revealed: how US and UK spy agencies defeat internet privacy and security" [online], *The Guardian.* September 06, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Bardin, J. (2011) "Ten Commandments of Cyber Counterintelligence", Adapted from Olsen, J. M. *"Ten Commandments of Counterintelligence"*, n.d.) *CSO Risk*. Posted on blog 2011-06-21. Retrieved on January 09, 2013 from of_cyber_counterintelligence_adapted_from_james_m_olson.

Clarke, R. M. (2004) *Intelligence Analysis: A Target-centric Approach*, CQ Press, Washinton D.C.
Bodmer, S. A. et al (2012) *Reverse Deception – Organized Cyber Threat Counter- Exploitation*, McGraw-Hill, New York.

Bodmer, S. A. et al (2014) *Hacking Back: Offensive Cyber Counterintelligence*, McGraw-Hill, New York.
Carrol, J. (2009) "Cyber Counter Intelligence", *Defense Tech*. Retrieved on December 03, 2012 from http://defensetech.org/2009/03/09/counter-cyber-intelligence/

Corbin, K. (2013) " 'Aurora' Cyber Attackers were really running Counter-Intelligence", *CIO*, Retrieved May 01, 2013 from http://www.cio.com/article/732122/_Aurora_Cyber_Attackers_Were_Really_Running_Counter_Intelligence?page=1&taxonomyId=3133

Dictionary.com (2014), *"counterintelligence"*, available at http://dictionary.reference.com/browse/counterintelligence

Duvenage, P. C. (2010). *Open-source Environmental Scanning and Risk Assessment in the Statutory Counterespionage Milieu*. Unpublished doctoral thesis. Pretoria, University of Pretoria.

Duvenage, P.C. (2013) "Counterintelligence," in Prunckun, H. (ed.), *Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries* (Springfield IL: Charles C. Thomas, 2013).

Duvenage, P.C. and Hough, M. (2011) "The Conceptual Structuring of the Intelligence and the Counterintelligence Processes: Enduring Holy Grails or Crumbling Axioms – Quo Vadis?". *Strategic Review for Southern Africa*, University of Pretoria, Pretoria.

Duvenage, P. C. and von Solms. S.H. (2013). "The Case for Cyber Counterintelligence" Paper read at *5TH Workshop on ICT Uses In Warfare and the Safeguarding of Peace (IWSP'13)*, Pretoria, South Africa. November.

Francq, A. (2001). "The Use of Counterintelligence, Security, and Countermeasures", in Fleisher F.S and Blenkhorn D. L (eds), *Managing Frontiers in Competitive Intelligence*, Quorum Books: Westport.

Farchi, J (2012). Offensive counter-intelligence and cyberwarfare—a paradigm shift in information security, ISACA, Retrieved from http://www.isaca.org/Knowledge-Center/Blog/Lists/ Posts/Post.aspx?List=ef7cbc6d%2D9997%2D4b62%2D96a4%2Da36fb7e 171af&ID=261

Giles, L. (2002) *Sun Tzu – The Art of War,* (Translation), Dover Publications, New York.

Godson, R. (2001) *Dirty tricks or trump cards - U.S. covert action and counterintelligence*. New Brunswick, Transaction Publishers.

Helton, D. (2013) "Human Threat and Cyber Counterintelligence – an Agent's Perspective", *Speartip*, November 26. Retrieved from http//www.speartip.com/ on January 04, 2014./

IBM (2013) *IBM Protects Clients from Security Attacks with New Cloud Solution,* 22 Oct 2013, [online] http://www-03.ibm.com/press/us/en/pressrelease/42269.wss

ISC^2 (2013) Michigan Chapter. *Events Diary*. November 8, 2013, [online], http://isc2chapter-westmi.org/category/events/

Kuusisto, R. and Kurkinen, E. eds. (2013) Proceedings of the12th European Conference on Information Warfare and Security, Jyväskylä (Finland), Academic Conferences and Publishing International Limited, Reading (U.K).

Lües, J. (2012). "IT security has failed – Once effective, It security is now deteriorating on all fronts." iWeek, Issue 225, June 06.

Meyer, H. E. (1987) *Real world intelligence*. Weidenfeld & Nicolson, New York.

Miller, N.S. (1980) "What is Counterintelligence – Discussants." in Godson R. ed. *Intelligence Requirements for the 1980's: Counterintelligence*. National Strategic Information Center, Washington (D.C.).

Nakashima, E. (2013), "To thwart hackers, firms salting there servers with fake data", The *Washington Post*, January 03.

Odom, W.E. (2003). *Fixing intelligence for a more secure America*. New Haven. Yale University Press.

Park, Y. and Stolfo, S. J. (2012). Software decoys for Insider Threat. Seoul. ASIACCS. http://ids.cs.columbia.edu/content/publications.html

Powell, D, Wick, A and Fergus, D. (2013) "Protecting against Cyber Threats" *Security Management*, (online), retrieved on May 11, 2013 from http://www.securitymanagement.com.

Prunckun, H (2012). *Counterintelligence: Theory and Practice*. Plymouth, Rowman & Little Publishers.

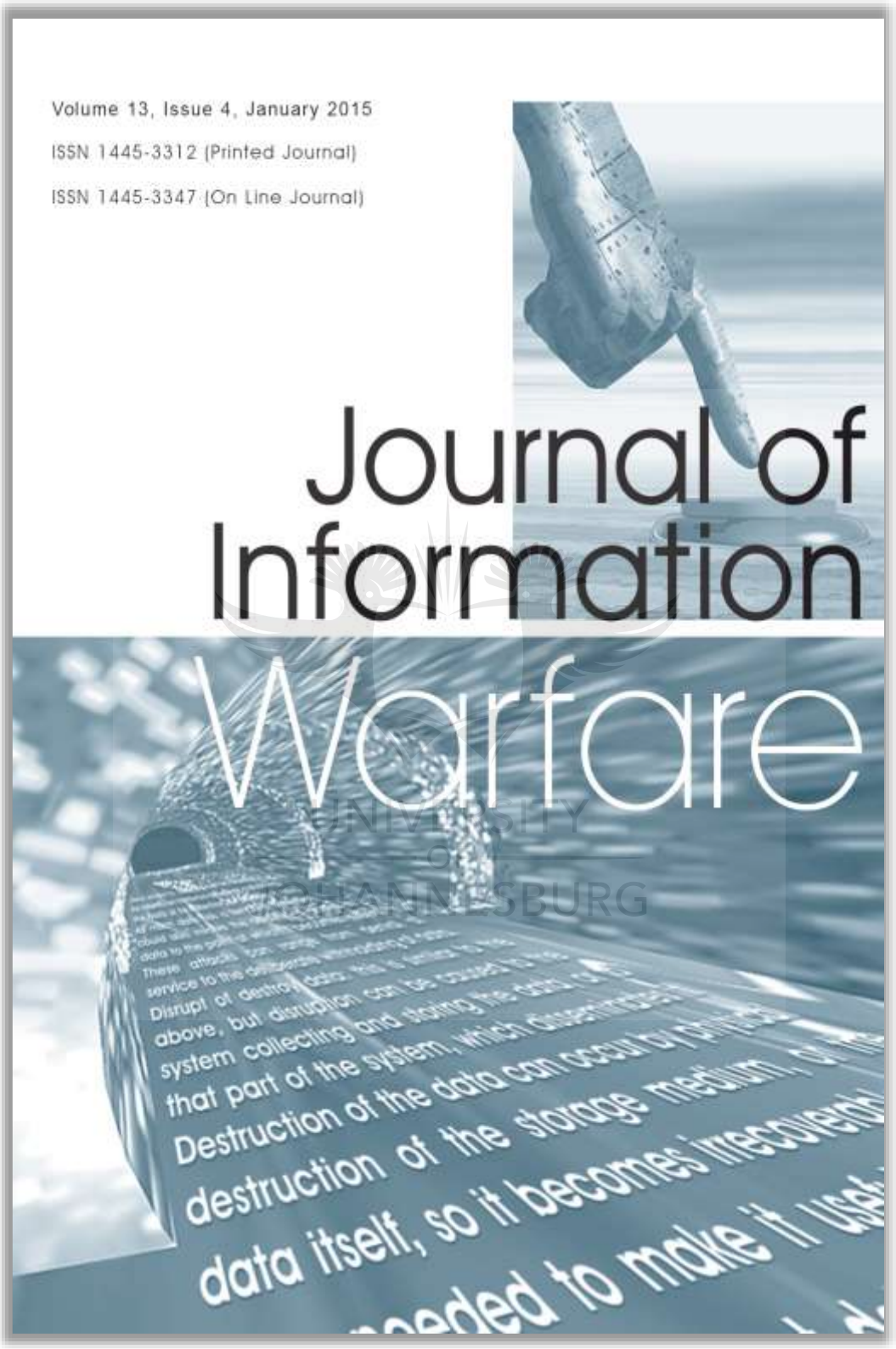
Sims, J. E. (2009) "Twenty-first-Century Counterintelligence" in Sims, J. E. and Gerber, B. (eds.) *Vaults, Mirrors and Masks – Rediscovering U.S. Counterintelligence*. Georgetown University Press, Washington (D.C.)

Van Cleave, M. K. (2007) *Counterintelligence and National Strategy*. School for National Security Executive Education. Washington (D.C.): National Defense University Press. Retrieved on July 02, 2010 from www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471485

Voris, J et al. (2013) *Bait and Snitch - Defending Computer Systems with Decoys*. Columbia University, New York.

World Economic Forum (2014) *Insight report - Global Risks 2014,*(online), www.weforum.org Global , WEF, Geneva.

ANNEXURE C



Cyber Counterintelligence: Back to the Future

PC Duvenage, SH von Solms

Centre for Cyber Security
Academy of Computer Science and Software Engineering
University of Johannesburg, South Africa
E-mail: duvenage@live.co.za;basievs@uj.ac.za

Abstract: *It is generally accepted that conventional cyber security generally has failed. As such, Cyber Counterintelligence (CCI) is fast gaining traction as a practicable approach to secure and advance our own interests effectively. To be successful, CCI should be an integral part of multi-disciplinary Counterintelligence (CI)–conceptually and in practice. With a view to informing sound CCI practice, this paper conceptualises CCI as a part of CI. It proceeds with going back to some time-tested CI constructs and applies these to the cyber realm. In so doing, this paper aims to offer a few building blocks toward a future of sound CCI theory and practice.*

Keywords: *Counterintelligence, Cyber Security, Cyber Counterintelligence*

Introduction

What was seen as a paradigmatic shift in thinking at the turn of this decade is now commonly accepted–that conventional cyber security which we have been relying on is deteriorating on all fronts (Lües 2012). As a result, cyber space is now probably more insecure than it has ever been (Bodmer *et al*. 2012). It is also likely to be the most secure than it is going to be for the foreseeable future. It is, simply put, going to get much worse. In this regard, the World Economic Forum's (WEF) 2014 Global Risk Report warned of "digital disintegration" when it stated: "The world may be only one disruptive technology away from attackers gaining a runaway advantage, meaning the Internet would cease to be a trusted medium for communication or commerce" (WEF 2014). The report continues by identifying the foremost "technological risks" for the immediate future as the breakdown of critical informational infrastructure and networks, an escalation of large scale cyber-attacks, and incidents of data fraud continue on an unprecedented scale (WEF 2014). Even early on in 2014, these were no longer risks but manifesting trends. Attesting to this concern is the continuing prominence in mass-media media reporting on the escalating detrimental impact of cyber criminals, hacktivists, and other role-players. Simultaneously, nation states' cyber surveillance by the intelligence apparatuses of not only the United States (US) and United Kingdom (UK), but also the People's Republic of China (PRC) and Russia continue to make headlines.

With the awareness of conventional cyber security's faltering, both state and non-state actors have been intensifying their quests for ways to more effectively protect and advance their cyber interests and, in the case of service providers and vendors, those of their clients. As could be expected, solutions offered in the marketplace vary considerably. Buzzwords and marketing slogans currently gaining favour include: counter exploitation, threat intelligence, offensive measures, hacking back, threatscape, and intelligence software analytics (IBM 2013; Helton 2013). Common to most of these solutions advocated, is recognition of the imperative of intelligence on threat actors and the need to engage threats pro-

actively/offensively. There is a sense of taking the fight to adversaries. The use of such notions and phrases would have been encouraging if it was indicative of more organisations "moving towards intelligence-driven risk management and decision-making models" (Helton 2013). As it currently stands, however, the use of these terms is, disturbing for three interrelated reasons. First, the terms are used vaguely and without the proper context from the statutory intelligence practice from which they are often derived. In marketing jargon 'intelligence' is used interchangeably with 'data and information'. Consequently, solutions offered under the rubrics of 'intelligence' may not solve the problems for which they purport to be the fix. In a similar vein, opting for quick-fix offensive actions, not dovetailed with an appropriately configured defensive posture, is inviting disaster. Equally disconcerting is the fact that solutions and terms are sometimes thrown around without due and categorical stipulations that some aspects of cyber defence and offense are the exclusive prerogative of the state apparatus in most countries. These functions ought not to be 'out-sourced' to other entities. Secondly, solutions being offered are essentially technical and tactical in nature. As important as they are, technical and tactical measures on their own are insufficient to confront the sophisticated threat actors about whom we are most concerned. Social engineering, to cite one example, "played a part in nearly every major hack or breach in 2013 yet it still stays in the background when we consider security controls. This is something that needs to change as we move forward" ([ISC]^2 2013). Thirdly, these solutions are presented as neat 'add-ons' or 'plugins' to be used as a layer additional to existing cyber security measures. 'Add-ons' seldom have, and certainly will not in the future offer adequate protection against advanced adversaries. For sizable institutions with significant digital and information interests to face up to such adversaries, cyber security needs to be a coherent part of their DNA and not mere feel-good plasters offering little real protection.

There is a way in which such synergy can be achieved and the tables turned on cyber adversaries. This paper posits cyber counterintelligence (CCI) as a practicable approach to effectively securing and advancing cyber interests. From this perspective, malicious cyber actions are not all bad news. The good news is that we can exploit malicious cyber actions to our advantage and to the detriment of the adversarial instigators. There is, however, a precondition: there can be no half measures. To be effective, CCI needs to be properly conceptualised and implemented. If not, it is likely to be self-defeating and could even end in self-destruction. For a substantial part, this conceptualisation entails the application of time-tested counterintelligence (CI) notions to the cyber sphere. It is a case of going back to counterintelligence fundamentals in order to enable our prosperity in the cyber sphere today and in the future. It is thus a case, as suggested by the paper's title, of going back in order to successfully move to a more secure cyber future.

This paper's primary aim is to provide a conceptual baseline that could help stimulate the academic discourse on CCI. Consequently, it ensues with a cursory overview of the status of CCI in the public and academic discourse on cyber security. An academic self-awareness of CCI's under-theorised status is, after all, a first step in addressing this near void. The paper proceeds with advancing CI and CCI constructs hopefully useful to this discourse. Rather than aiming to advocate radically new concepts, the emphasis is on presenting existing knowledge in a manner conducive to further academic debate. Such conceptual 'building blocks' include a definition and delineation of the CI as a CCI sub-discipline, a taxonomy for CCI methods and means, as well as a CCI matrix for configuring an offensive-defensive posture. It concludes with some views on CCI's future by suggesting areas for further academic enquiry.

As noted above, the following section reflects on CCI under-theorised status, since such awareness is an important first step in make progress with the academic discourse.

Cyber Counterintelligence's under-Theorised Status

In one form or the other, cyber counterintelligence has been practised as part of the statutory counterintelligence functions in various intelligence communities for well over two decades. CCI has also been offered as a service provided by a few niche companies for well over a decade. Until very recently, however, CCI has not really gained traction outside the statutory security structures and the small batch of clients the niche companies served. Despite the key it holds to secure cyber interests for state and non-state actors, CCI entered the second decade of the 21st century underappreciated and underexplored in policies and in the literature in the public domain. The overwhelming majority of governments' cyber security policies do not make any references to counterintelligence. And, in the few instances that the concept is cited, counterintelligence is hardly at the centre.

Anecdotal indications are that CCI has fast been gaining traction during the last two years. The 2013 proceedings of the 12th European on Cyber Warfare and Security (ECCWS), for example, consist of 44 papers and are 406 pages long (Kuusisto & Kurkinen 2013). Not one of these papers makes mention of CCI. There is, in fact, only one sentence in the whole of the proceedings that makes cursory reference to the general concept of counterintelligence (Kuusisto & Kurkinen, 2013). A mere one year later, and ECCWS 2014 featured a dedicated mini-track to Cyber Intelligence/Counterintelligence. While this certainly reflected an increased awareness of CCI, contributions remain scarce. Only one paper presented at ECCWS 2014 had CCI as focus or had 'counterintelligence' in its title.

While a few commendable books have been published on the subject, these are minuscule in comparison with the proliferating material on cyber security in general. The shift in emphasis towards CCI is nonetheless also apparent here. An outstanding work by Bodmer *et al.* was first published in 2012 with the title *Reverse Deception – Organized Cyber Threat Counter-Exploitation* (Bodmer *et al*. 2012). The edition due for release in 2014–which, as far as could be surmised from pre-launch advertising, retains the core of the 2012 edition–is more aptly called *Hacking Back: Offensive Cyber Counterintelligence* (Bodmer *et al*. 2014).

Although CCI is poised to gain prominence, the participation in and agenda of this discourse will inevitably be influenced by the relative obscurity of CI in general. CCI will be demonstrated in further sections as a sub-set of the broader, multi-faceted CI discipline. It thus follows that contributions to CCI would need to be preceded by some grounding in CI. CI, however, (and herein lies the glitch), is in itself academically obscure and underappreciated. This obscurity is as old as its inception as a formalised discipline in the run up to World War II. Some would argue that this can be ascribed to the fact that a large part of CI work relies for its effectiveness on secrecy. Yet, we do not need to reveal secrets to talk seriously about matters of Intelligence and Counterintelligence (Meyer 1987). A more likely reason for CI's obscurity in the academic debate is to be found in the fact that it is arguably the most complex and least understood of all Intelligence disciplines (Godson 2001). The following statement by a U.S. CI veteran in the midst of the Cold War has lost none of its relevance: "It is not easy, nor can one feel confident, to re-enter this world where, it has been said, the tortuous logic of counterintelligence prevails...Unfortunately, there seems to be no easy way to explain counterintelligence...Because effective counterintelligence is a combination of so many aspects" (Miller 1980). Even among policy makers, scholars and 'national security practitioners' in foremost intelligence communities such as those of the

U.S., “the role of counterintelligence remains little known or understood” up to this day (Van Cleave 2007).

Since the role, functions and importance of CI is opaque within statutory intelligence circles, the reluctance of ‘techies’ to apply this concept to the cyber sphere is understandable. In a similar vein, those skilled and experienced in more conventional counterintelligence do not necessarily have a sound working knowledge of technical cyber. If we are not clear on a conceptual level, we can hardly make progress in the academic discourse, thereby eventually affecting our ability to implement sound solutions. In the conceptual difficulties of CI also lies the opportunity. If we can understand and explain CI, we can explain CCI and then we can unlock the latter’s potential as a force multiplier.

This section illustrated the need for contributions to the budding CCI field to be clearly rooted in CI. In line with this contention, the next section provides a conceptual primer of CI.

A Primer on Counterintelligence

Counterintelligence has been practised and described for millennia. Some enduring principles were penned in 500 B.C. by the much-quoted Sun Tzu in a specific chapter in his *The Art of War* devoted to the use of spies and counter-spies (Giles 2002). The term in its contemporary connotations entered the English lexicon in the mid-1930s (Dictionary.com 2014). For some, counterintelligence is all about spies outgunning adversarial spies. For others, it invokes mundane security measures such as computer passwords, restrictions on the use of computing equipment, security guards, access control, and the like. Counterintelligence is all of these things, and so much more (Duvenage & von Solms 2013).

Delineating Counterintelligence

Counterintelligence can be defined as the collective of measures undertaken to identify, deter, exploit, degrade, neutralise, and protect against adversarial intelligence activities deemed as detrimental or potentially detrimental to one’s own interests (Duvenage 2010). The term ‘counterintelligence’ is thus an abbreviated form for the countering of hostile intelligence activities. Adversaries engaging in hostile intelligence actions include nation states, corporate entities, criminals, activists, individuals, and any combination of these.

Adversarial intelligence activities include espionage, deception (disinformation), influencing, and some other forms of covert action that can have disruptive and destructive outcomes. Of these different intelligence activities, espionage is the most central. Espionage to obtain protected information in order to gain a competitive advantage can be an end in itself; or such information can be used to further other malicious ends such as data manipulation, disinformation, and disruption. Sophisticated adversaries execute their intelligence actions through the exploitation of humans (HUMINT) and technical means (TECHINT). The latter, in turn, comprise Signal Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT), and Cyber Intelligence (CYBINT). These conduits and their relation to adversarial intelligence ends are graphically depicted in **Figure 1**:

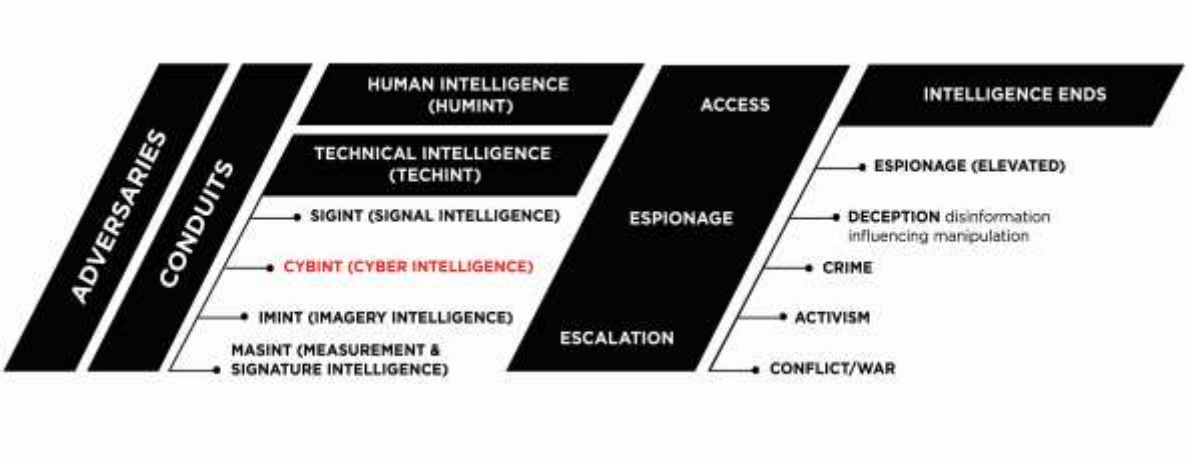


Figure 1: Adversarial Intelligence: Conduits and Ends

Several revelations by the whistle-blower Edward Snowden provide a practical illustration of the above. During September 2013, for example, *The Guardian* newspaper revealed that the British and U.S. Agencies run HUMINT operations to "help secure an insider advantage" (Ball, Borger & Greenwald 2013). To this end the British Government Communications Headquarters (GCHQ) established a HUMINT Operations Team (HOT) "responsible for identifying, recruiting and running covert agents in the global telecommunications industry" (Ball, Borger & Greenwald 2013). These operations enabled the Agency to "tackle some of its most challenging targets", specifically, in as far as the breaking of encryption was concerned (Ball, Borger & Greenwald 2013). In this instance, success in the field of CYBINT thus depended on the effectiveness of HUMINT operations. The reverse is of course also true. Given the high and growing digital dependence, CYBINT is often a critical enabler in the HUMINT sphere. To be effective, CI needs to counter all types of adversarial intelligence activities and, in the case of high-end adversaries, it has to do so in more than one of or in all of the conduits.

Counterintelligence: Measures, Means, and Modes

In order to execute its mission, CI relies on measures and means that vary from passive-defensive to active-offensive ones. At the one end of the spectrum, passive-defensive measures strive to deny adversaries access to protected information assets. They aim to reduce vulnerabilities through a combination of policies, procedures, and practices– sometimes referred to on a lighter note as "gates, guards, guns, and dogs" (Francq 2001). Apart from denying opponents access, properly instituted passive-defences measures are like caste walls. In addition to preventing common intrusions, their presence discourages intrusion attempts and consequently serves a deterrence function. Examples of passive-defensive measures are access and movement control, perimeter security, alarm systems, safes and vaults, fire prevention measures, key control, and the control of the removal and transfer of information from facilities where valued information is located. At the other ends of the spectrum, offensive counterintelligence aims to neutralise a competitor's intelligence efforts through measures ranging from deception and manipulation to the neutralisation of adversarial intelligence activities and systems. Deception takes various forms and can be achieved through numerous means. Skilfully executed, deception attains a primary counterintelligence aim, which is the manipulation and control of an adversary. This is aptly encapsulated by Codevilla (1992) when he states "Action against the enemy through the enemy's own intelligence is the very consummation of CI". There are of course also aggressive CI measures that CI shares with its sister--discipline, Covert Action. Under certain

conditions, assassinations and even extraordinary rendition can be classified as active-offensive CI neutralisation measures (Duvenage 2010).

Between passive-defensive and active-offensive lies a wide array of other measures, such as: pre-employment personnel security; in-service personnel security; technical surveillance countermeasures (TSCM); encryption; surveillance (physical, static, mobile, and electronic); double agents; agents; and continued monitoring. In most instances, these measures can serve defensive or/and offensive purposes. Defensive counterintelligence tactics and strategies provide information to and act as triggers to alert the offensive side of the practice. Similarly, offensive operations (for example a source reporting on an adversary's intentions and capabilities) inform the proactive configuration of defences. It will also be noted that several of these are highly useful in the collection of information of internal vulnerabilities (such as organisational weaknesses and insider threats), the external environment, as well as actual and potential adversaries. It goes without saying that, without such information being analysed, CI would be blind and unable to execute the defensive-offensive interplay. The following matrix, depicted in **Figure 2**, is somewhat of an over-simplification, but is nonetheless useful in conveying the nuanced nature of the offensive-defensive interplay as well as the importance of collection:

<table>
<tr><th colspan="2">Defensive Mode
Denies adversaries access to and generates information about adversaries</th></tr>
<tr><td>Passive Defence
Denies the adversary access to information through physical security measures and security systems.</td><td>Active Defence
The active collection of information on the adversary to determine its sponsor, modus operandi, network, and targets. Methods include physical and electronic surveillance, dangles, double agents, moles, and electronic tapping.</td></tr>
<tr><th colspan="2">Offensive Mode
Aims to manipulate, degrade, control and neutralise adversaries</th></tr>
<tr><td>Passive Offensive
Reveals to the adversary what you want them to see. This could range from selective exposure of actual information to decoys and dummies. The adversary is thus left to draw its own inferences and interpretations.</td><td>Active Offensive
The adversary is fed with disinformation and its interpretation thereof manipulated. Disinformation can be channelled through, for example, double agents and 'moles'. Active-offensive CI could include some forms of covert action. Covert action, in its use here, denotes the targeting of an adversary through the influencing of events, conditions, individuals, groups, or institutions to the benefit of a sponsor in a manner not attributable to the sponsor or by offering plausible deniability. Influencing is achieved through measures that vary from paramilitary and political actions to propaganda and intelligence assistance.</td></tr>
</table>

Figure 2: A Four-Sector Counterintelligence Matrix (Compiled by the authors on the basis of narratives in Prunckun 2012; Sims 2009; Odom 2003; Godson 2001)

Counterintelligence Process

The preceding matrix and discussion above demonstrate that CI is an intricate and exhaustive discipline. It is not only about defences, but is also about the concrete advancement of one's own interest vis-à-vis adversaries' interests. It could be surmised from the above, no matter how well-resourced, the CI endeavour cannot protect all assets or advance all interests all the time. The bodies of information that justify CI protection as well as the systems, processes, institutions, and individuals in which such information resides must be identified and prioritised (Prunckun 2012). Since offensive action carries even higher risks and costs, CI should be crystal clear on it role in this regard. Such clarity in turn presupposes CI to be in

synergy with Intelligence and at the centre of a government's or business' strategy. These are the critical roots of the CI premise.
While few would dispute CI's premise, opinions are divided on the structuring of the CI process. This paper favours a process model that differs fundamentally from the traditional (positive) intelligence cycle and Clarke's target-centric process (Clarke 2004). This process model comprises the following steps (Duvenage & Hough 2011; Duvenage 2013):

1. Identify information and assets that warrant the expending of counterintelligence resources.
2. Assess vulnerabilities that increase the risk of information being compromised.
3. Scan the environment and identify actual or potential threat-agents.
4. Collect information on threat-agents and appraise the risks.
5. Re-assess own vulnerabilities and review defences.
6. Develop sets of counterintelligence measures and projects (offensive and defensive).
7. Implement the recommended countermeasures and projects.
8. Continually assess and adapt the implemented countermeasures to compute the changing environment.

The apparent simplicity of this model in certain respects masks some intricacies of the counterintelligence process. In the case of offensive counterintelligence, for example, espionage adversaries will be engaged through a pattern of activities interwoven within the broader counterintelligence processes. Offensive counterintelligence, in other words, will be performed as a sub-process of step 6 outlined above. This sub-process draws an important distinction between an 'espionage adversary' and an 'espionage target'. An 'espionage adversary' is the ultimate sponsor of an intelligence effort, while the counterespionage target is the instrument with which intelligence activities are conducted. This instrument is targeted by an opposing entity's counterespionage structure–hence the phrasing 'counterespionage target'. A nation state and its intelligence service would, for example, be espionage adversaries and the proxies for conducting the actual espionage would be the counterespionage targets. Such proxies could be recruited agents or third entities (for example, front companies). Employing this distinction, the offensive counterespionage process–which is executed per step 6 of the process model above - will typically have the following sub-steps (Duvenage & Hough 2011):

6.1 Identification of espionage adversaries.
6.2 Prioritisation of espionage adversaries.
6.3 Investigation of espionage adversaries.
6.4 Engagement of counterespionage targets.
6.5 Exploitation of counterespionage targets.
6.6 Neutralisation of targets and termination of operation

This section provided a primer that demarcated CI, explained CI measures and modes, and offered changes to the CI process. Building on this overview of CI, the paper proceeds with conceptualising CCI.

Conceptualising Cyber Counterintelligence

This section provides a provisional definition of CCI, advances a model for integrating CCI with CI and Intelligence, and outlines some CCI methods, means, and modes.

Defining and Delineating Cyber Counterintelligence

While various definitions for CCI have been advanced, none of these specifically explicate the relationship between CCI and CI (for example, Carrol 2009; Bodmer *et al*. 2012; Farchi 2012). In keeping with the paper's central contention, CCI is defined as that subset of multi-disciplinary CI aimed at deterring, preventing, degrading, exploiting, and neutralising adversarial attempts to collect, alter or in any other way to breach the C-I-A of valued information assets through cyber means. Expanding on this definition, it is postulated that CI delineates CCI on the following three tiers (Duvenage & von Solms 2013):

- Applied to the cyber context, CI theory and practice provides a conceptual template for modelling CCI actions in the safeguarding and advancing of cyber interests. Mirroring CI, CCI has offensive and defensive missions that are distinguishable but not separable.
- To be effective, cyber counterintelligence needs to be interlocked with all-field counterintelligence–defensively and offensively. In this sense, CI cements an integrated approach to securing the cyber space. CCI is thus about both the modelling of cyber actions on CI, and the integration of these offensive and defensive actions with conventional CI.
- Effective CI protects and promotes the intelligence endeavour and business strategy. Since CCI is part of CI, it is also integrated in business strategy and intelligence.

Figure 3 depicts this three-tiered relationship graphically.

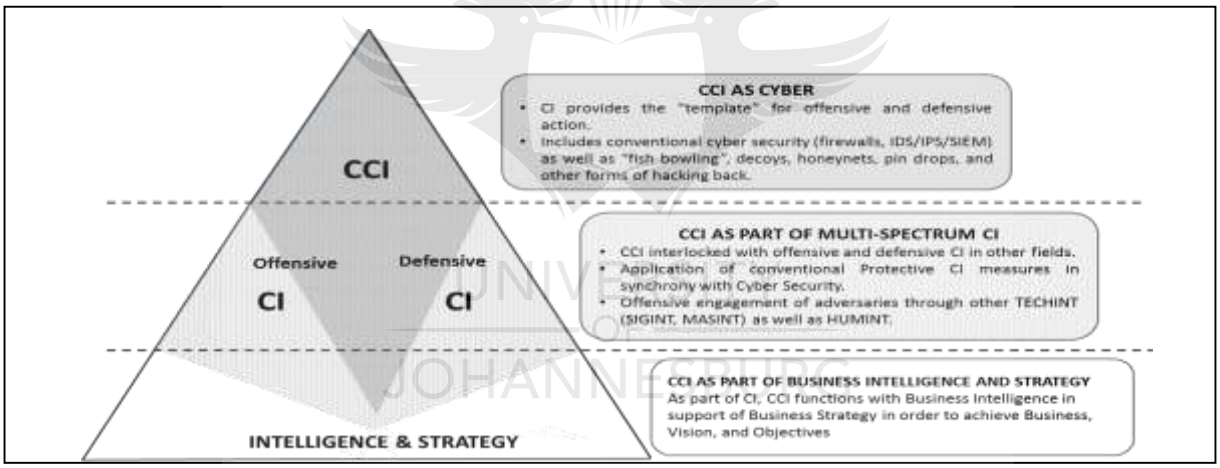


Figure 3: The Cyber Counterintelligence Pyramid

The postulation, per the narrative and **Figure 3**, is admittedly cursory and does not purport to conform to the criteria of a conceptual model. However, it could provide a useful premise for further research and for the development of a conceptual model for implementation in the cyber domain.

Overview of Cyber Counterintelligence Methods, Means, and Modes

The section above discussed defensive and offensive CCI actions. Mirroring CI in general, CCI methods and means can be deployed in offensive and defensive modes, but defy categorisation in watertight compartments. At the very ends of this spectrum there are a few methods and means that could be designated clearly as active-offensive (notably cyber weapons with a destructive purpose, such as Stuxnet) or passive-defensive (for example, access control and validation directives). In the main, however, offense-defensive and active-

passive are not neat compartments, but rather the manner in and end towards which methods and means are deployed (Duvenage & von Solms 2013). This is illustrated in the following matrix, **Figure 4**, which depicts the four cyber-counterintelligence modes (postures) an entity could assume:

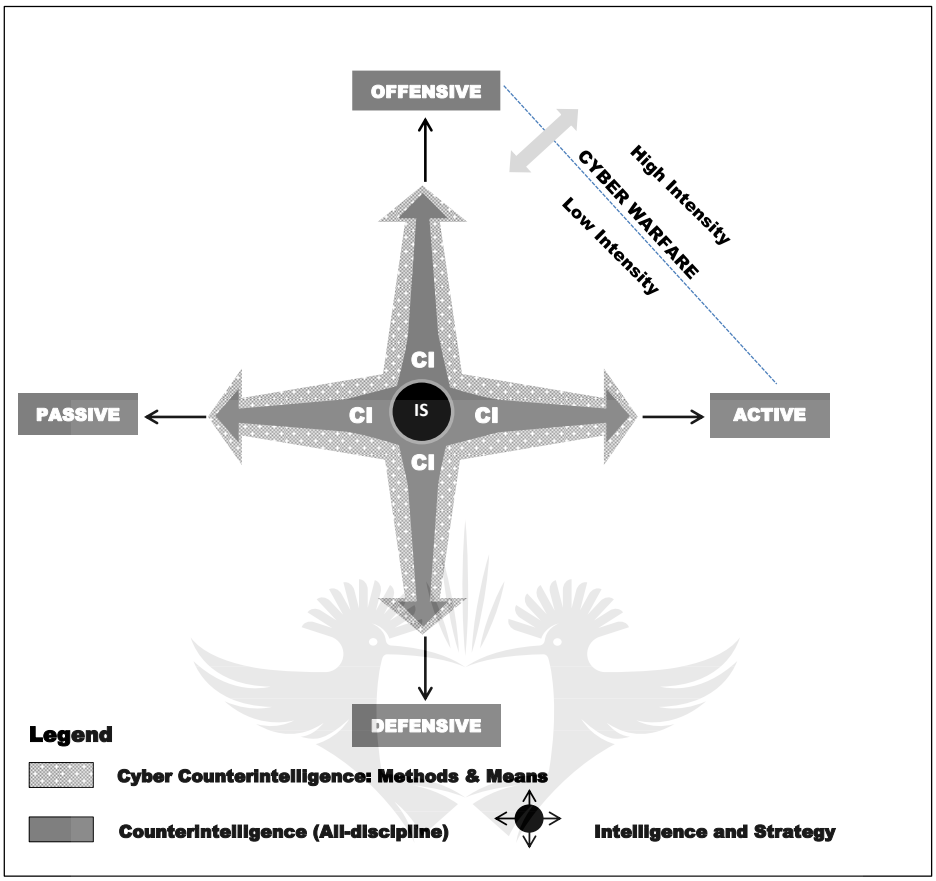


Figure 4: Cyber Counterintelligence Matrix

The CCI matrix per **Figure 4** is more than a notional construct and can be applied practically by entities (with sizable cyber interest and assets) in the plotting of CCI methods and means. The matrix ensures that a presence is maintained or, at the very least, that contingency planning is done with respect to all four quadrants. It furthermore facilitates innovation and creativity in the application of methods and means–within legal parameters, of course. Contrary to a misconception, for example, an Intrusion Prevention System can be configured with surprising positive results in executing aims in the other three quadrants. Consequently, the construction of a tabulated taxonomy of CCI methods and means could very well be an oversimplification. Even more so should the taxonomy endeavour to point to parallels that exist between CCI measures and those in CI generally. Nonetheless, at this early stage of conceptualising CCI, such a simplification can serve as a jumping off point for further debate. With this caveat, a cursory taxonomy of CCI methods and means is provided in **Table 1**:

Table 1: Taxonomy of Cyber Counterintelligence Methods and Means (Duvenage & von Solms 2013)

<table>
<tr><th colspan="3">DEFENSIVE MODE</th></tr>
<tr><td colspan="3">Passive ⟶ Active</td></tr>
<tr><td>Deny >></td><td>Detect >></td><td>Collect</td></tr>
<tr><td>Physical Defensive</td><td>Personnel/User Defensive</td><td>System Defensive</td></tr>
<tr><td>Protects against:
Unauthorised access to facilities and systems.
In loco theft of data, hardware.
Introduction of malware through physical access to systems.
Physical destruction.
Unauthorised reading (acoustic, visual, analogue, signals).
While not conventionally seen as a Physical Defence, supply-chain management has a physical defensive function. It is also part of System Defences.
<u>Remark</u>: Within the area of Physical Security, there is an extensive and strong convergence between CCI and conventional CI. In keep with the article's central contention that CCI ought be seamlessly integrated with CI, the sub-category 'Physical Defensive' is included in this taxonomy. Note is taken of the fact that with other classification criteria some of the measures listed above may be excluded from CCI, per se.</td><td>Consists of aspects such as
IT and user personnel vetting, re-vetting, and confidentiality agreements.
Personnel security measures, BYOD user parameters, or exclusions.
User programmes in cyber security which cover policy and procedures for the handling of security incidents and malfunctions.
Overlapping with system defences, the use of software decoys to mitigate the insider threat.
Investigations focused on cyber security incidents involving personnel. Could also include digital forensic investigations.</td><td>Comprises a combination of
Hardware and software such as
✓ Network perimeter-based security (filters, certain firewalls, etc.).
✓ Malware scanners.
✓ Integrated automated systems/tools (that collect and evaluate information about devices connected to a network, activities thereon–inclusive of intrusions). Examples of such tools, discussed further on in the table, are decoys and honeynets.
✓ Overlapping with the latter, are IDS and IPS. Depending on its configuration, a honeynet can be defensive or offensive in type/mode. The term fish bowling denotes the defensive configuration. (Remark: See http://ids.cs.columbia.edu/content/publications.html for extensive work that has been done on IDS/IPS).
Processes (such as supply-chain management, product verification, and testing) are also, in part, system defences.
Vulnerability assessments and penetration testing.
Incident investigation and response. A CERT is, by definition, defensive–although it might contain offensive elements in its responsive action.
BYOD regulation in as far as network interfacing is concerned (also part of Personnel Defenses).</td></tr>
<tr><td rowspan="2"></td><td colspan="2">• The use of honeynets and software decoys to mitigate the insider threat creates an overlap between personnel and system defensive measures. They are mostly active CCI means.</td></tr>
<tr><td>• Investigations focused on internal cyber security incidents involving personnel. May include digital forensic investigations.</td><td>• Investigations of external cyber intrusions could be part passive and part active system defence.</td></tr>
</table>

OFFENSIVE MODE		
Passive →		***Active***
Collect >> ***Disrupt***	>> ***Exploit***	>> ***Destroy***
• **Collection** of information on and the monitoring of the cyber sphere to detect cyber adversaries and their exploitation of the cyber sphere in a manner that is not own-network restricted (i.e., which require more than deployment of systems described under defensive mode). Could, depending on configuration, also include IDS/IPS, honey-client applications (as opposed to host-based honeypots) and data mining. • The recruitment and handling of **virtual agents** on underground forums (under true or false flag) that can serve the purpose of collection and/or exploitation. (Under certain circumstances virtual agents can also develop into HUMINT assets).	Measures taken to **exploit** and to **neutralise** adversaries' activities in the cyber sphere: • **System and honeynet** can be **configured offensively** with the aim of exploiting and deceiving adversaries. False information is displayed to adversarial reconnaissance tools, network scanners, and listeners, etc. This has as one of its aims to lead adversaries in the direction of your own preference. • Utilisation of **virtual agents** for offensive purposes.	**Cyber warfare**, in the full extent of the term, is typically excluded from the mandate of civilian intelligence communities. A cyber warfare capability should be flexible and should allow utilisation without, or in conjunction with, kinetic war. Nevertheless, a top class civilian CCI outfit will need to have the authority and the capacity to very selectively conduct operations that have cyber warfare characteristics. Such cyber CCI operations will share characteristics with covert action. (Covert action aims to influence role-players, conditions, and events without revealing the sponsor's identity.) Within business, the use of offensive measures will be determined by the legal and regulatory framework within which the entity operates.
• **Cyberespionage** on adversaries. Distinguishable from own-system collection (IPS, IDS, honeynets) on the basis that adversarial networks are actively targeted and exploited in accordance with strategic and operational objectives.		

Table 1 samples only some of the possible CCI methods and means. Moreover, and given the length constraints of an article, only a very few of these are further elaborated upon, namely honeypots and decoys, cyber profiling, and cyber-agent operations.

In the means cited above, honeynets feature prominently in the active and passive as well as the defensive and offensive modes. Honeynets have been in use for more than two decades with the principle objective to detect, to monitor, and to gain intelligence on adversarial intrusion on a network (Bodmer *et al*. 2012). In recent years, the purposes of honeynets diversified from its original mostly defensive use to include also a much more active and/or offensive role. Concurrently, the different types of honeypots and configurations are sharply increasing. In as far as architecture goes, and depending on specific needs and situations, honeynets can be centralised, distributed, federated, and confederated (Bodmer *et al.* 2012). The diversifying aims of honeynets now include one or a combination of deception, disinformation, and the draining of adversarial resources through labyrinths and "rabbit holes" (Nakashima 2013; Duvenage & von Solms 2013). In a similar vein, decoys are highly useful in disrupting external intrusion and/or mitigating the insider threat (Voris *et al*. 2013). The more resourced and sophisticated the adversary, the greater the imperative to attune the staging of honeynets and the content filling of honeypots, honeyfiles, and honeytokens in accordance with the opposition's interests and modus operandi (Duvenage & von Solms 2013).

Counter-action with matching sophistication, in turn, requires sound analysis of high-grade information on the environment and on adversaries. Unsurprisingly, cyber profiling, which involves the application of criminal and intelligence profiling methods to the cyber realm, is fast gaining field as a CCI specialisation area (Bodmer *et al*. 2012). In order to procure information on actual and potential adversaries, as well as to keep to tabs on hacking communities of all sorts, CCI outfits maintain a layered presence on nets and forums. This presence varies from the deployment of soft and hardware instrumentalities to the cyber equivalent of HUMINT counterespionage, namely the recruiting, turning, and handling of witting/unwitting agents (Duvenage & von Solms 2013).

Cyber Counterintelligence as a Multi-Disciplinary Subset of Counterintelligence

In line with the theoretical outline of the relationship between CCI and CCI (**Figure 3** and **Figure 4**), the practical safeguarding and advancement of cyber interests is a multi-disciplinary endeavour. CCI is thus not only multidisciplinary in itself but is overlaid upon multi-disciplinary counterintelligence. This multi-disciplinary mind set is especially relevant in the face of sophisticated threats. As part of the Edward Snowden revelations it was reported, for example, that the USA and UK Intelligence communities rely on the recruitment and running of HUMINT sources networks in the global telecommunications industry to "tackle" some of their "most challenging targets"-inter alia in the cryptology field (Ball, Borger & Greenwald 2013). In keep with such multi-dimensional threats, a CI operation in the cyber field could entail a multi-disciplinary team comprised of cyber security specialists, strategic analysts, tactical and technical analysts, HUMINT specialists (such as agent handlers and intelligence psychologists), cyber defense technical experts, language experts, ethical hackers, sociologists, and religious experts (Bardin 2011). While a sharp edge on the offense, humans are also the weakest and possibly the most ruinous chink in the defensive armour. Powell, Wick and Fergus (2013) assert "an organization's insiders" are "primary threats to cybersecurity … [which are] ….the most difficult to mitigate". Complementary to technical defences, CI personnel fidelity measures, and HUMINT counterespionage practices are thus critical. This is being highlighted by unfolding detail around the Edward Snowdon breach.

The convergence of cyber and HUMINT counterintelligence was furthermore demonstrated by a recent re-evaluation of the Aurora attacks. This re-evaluation suggests the Aurora attacks were not, as was initially thought, a People's Republic of China (PRC) operation targeting human-rights activists. It was in fact a Chinese counterintelligence operation to determine whether PRC intelligence operations and agents had been compromised by USA intelligence (Corbin 2013). Duvenage & von Solms (2013) cite as a further example of "an integrated CI initiative, a disinformation campaign as part of which the staging and content filling of a honeynet is harmonised with disinformation fed to an adversary through a HUMINT asset (e.g. double agent)".

Cyber Counterintelligence and Counterintelligence–An Integral Part of Intelligence and Strategy

To re-state the paper's recurring theme, CCI forms part of and is guided by the integrated CI endeavour. Consequently, CCI follows the CI processes discussed in Section 3.3. The CI processes, in turn, ought to function in synergy with positive intelligence. CI not only safeguards intelligence operations, but also renders inside information on competitors highly useful to executives. In addition, deception, disinformation, and other such projects support a

company in achieving its business objectives. This is thus a more a practical illustration of the theoretical postulations per **Figures 3** and **4** which put business objectives and strategy as the pivot around which CI and CCI evolve.

Conclusion

This paper forms part of a still spare yet fast-growing body of academic literature which views CCI as a practicable approach for governments, businesses, and other sizable entities for securing and for advancing cyber interests. Proliferating threats and trends affecting cyber security are not all bad. Contradictory as it may appear, the more extensive adversarial cyber action the greater the potential opportunity could be for counter-exploitation. The call for cyber CCI should not be misconstrued as a call for a free-for-all cyber Wild West. Performed haphazardly and in a silo, CCI is could be self-destructive.

There are several pre-conditions for effective CCI. To be effective, CCI should be an integral part of multi-disciplinary CI–conceptually and in practice. In academic literature, however, such conceptualisation is lacking. For the most part researchers have endeavoured to progress with CCI theory construction, without a sound foundational explication of CI. Theory so formulated and models so constructed could hold serious negative repercussions on a practical level. Within counterintelligence, the price for bad theory is eventually costly failures. As pointed out in an earlier contribution: "Conceptual models are not mere theoretical, academic constructs. Models condition our thinking and our approach to practice. What we therefore need is a sound overarching CCI model that can synergistically bind developing theory" (Duvenage & von Solms 2013).

Therefore, this paper aimed to put the counterintelligence in cyber counterintelligence. This was done through conceptualising CCI as part of multi-disciplinary CI and the applications of time-tested CI constructs to the cyber sphere. Secondly, the article offered a few conceptual constructs as the beginning of the construction of such a model. In so doing, it demonstrated the degree to which conventional, time-tested CI constructs can guide CCI's conceptualisation. The actual construction of a credible model, however, will require extensive in-depth, multi-disciplinary research and debate.

References

Ball, J, Borger, J & Greenwald G 2013, 'Revealed: how US and UK spy agencies defeat internet privacy and security', *The Guardian*, viewed 30 Sept. 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security/>.

Bardin, J 2011, 'Ten commandments of cyber counterintelligence', as adapted from Olsen, J *'Ten Commandments of Counterintelligence'*, viewed 09 Jan. 2013, <http://www.csoonline.com/article/2136458/identity-management/ten-commandments-of-cyber-counterintelligence---adapted-from-james-m--olson.html>.

Clarke, R 2004. *Intelligence analysis: A target-centric approach*, CQ Press, Washington, D.C.

Bodmer, S, Kilger M, Carpenter, G & Jones, J 2012. *Reverse deception–Organized cyber threat counter- exploitation*, McGraw-Hill, New York.

Bodmer, S et al 2014. *Hacking back: Offensive cyber counterintelligence*, McGraw-Hill, New York.

Carrol, J 2009, 'Cyber counter intelligence', *Defense Tech*, viewed 03 Dec. 2012, <http:// defensetech.org/2009/03/09/counter-cyber-intelligence/>

Codevilla A 1992. *Informing statecraft–intelligence for a new century*, The Free Press, New York.

Corbin, K 2013,''Aurora' cyber attackers were really running counter-intelligence', *CIO*, viewed 01 May 2013, <http://www.cio.com/article/732122/_ Aurora_Cyber_ Attackers_Were_Really_Running_Counter_Intelligence?page=1&taxonomyId=3133>.

Dictionary.com, 2014 '*counterintelligence'*, viewed 13 Jan. 2014, <http://dictionary.reference.com/browse/ counterintelligence>.

Duvenage, P 2010, 'Open-source environmental scanning and risk assessment in the statutory counterespionage milieu', Ph.D. dissertation, University of Pretoria.

Duvenage, P 2013. "Counterintelligence," in Prunckun, H (ed.), *Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries*, Charles C. Thomas, Springfield IL.

Duvenage, P & Hough, M 2011, 'The conceptual structuring of the intelligence and the counterintelligence processes: Enduring holy grails or crumbling axioms–*quo vadis*?' *Strategic Review for Southern Africa*, University of Pretoria, Pretoria.

Duvenage P & von Solms, S 2013 "The case for cyber counterintelligence", *5TH Workshop on ICT Uses in Warfare and the Safeguarding of Peace*, IWSP'13, Pretoria.

Francq, A 2001, 'The use of counterintelligence, security, and countermeasures', eds. F Fleisher & D Blenkhorn, *Managing Frontiers in Competitive Intelligence*, Quorum Books, Westport.

Farchi, J 2012, 'Offensive counter-intelligence and cyberwarfare—a paradigm shift in information security', *ISACA*, viewed 11 Nov. 2012, <http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?List=ef7cbc6d% 2D9997%2 D4b62%2D96a4%2Da36fb7e 171af&ID=261>.

Giles, L 2002. *Sun Tzu–The Art of War*, (Translation), Dover Publications, New York.

Godson, R 2001. *Dirty tricks or trump cards--U.S. covert action and counterintelligence*, Transaction Publishers, New Brunswick.

Helton, D 2013, 'Human threat and cyber counterintelligence–An agent's perspective', *Speartip*, viewed 4 Jan. 2014, <http//www.speartip.com/ >.

IBM 2013, *IBM Protects Clients from Security Attacks with New Cloud Solution*, viewed 22 Nov. 2013, <http://www-03.ibm.com/press/us/en/pressrelease/42269.wss>.

(ISC)^2 Michigan Chapter 2013, *Events Diary*, 8 Nov. 2013, viewed 2 Jan. 2014, < http://isc2chapter-westmi.org/category/events/>.

Kuusisto, R & Kurkinen, E, (eds.), 2013, *Proceedings of the12th European Conference on Information Warfare and Security, Jyväskylä (Finland),* Academic Conferences and Publishing International Limited, Reading.

Lües, J 2012, 'IT security has failed–Once effective, ITsecurity is now deteriorating on all fronts', *iWeek*, no. 225, 6 June 2012.

Meyer, H 1987. *Real world intelligence*, Weidenfeld & Nicolson, New York.

Miller, N 1980. ‘What is counterintelligence–Discussants’, ed. R Godson *Intelligence requirements for the 1980’s: Counterintelligence*, National Strategic Information Center, Washington, D.C.

Nakashima, E 2013, ‘To thwart hackers, firms salting their servers with fake data’, *The Washington Post*, 3 Jan. 2013.

Odom, W 2003. *Fixing intelligence for a more secure America*, Yale University Press, New Haven, CT.

Powell, D, Wick, A & Fergus, D 2013, ‘Protecting against cyber threats’, *Security Management*, viewed 11 May 2013, <http://www.securitymanagement.com.>.

Prunckun, H 2012. *Counterintelligence: Theory and practice*, Rowman & Littlefield Publishers, Plymouth, UK.

Sims, J 2009, ‘Twenty-first century counterintelligence’, eds. J Sims & B Gerber, *Vaults, mirrors and masks–Rediscovering U.S. counterintelligence*, Georgetown University Press, Washington, D.C.

Van Cleave, M 2007, *Counterintelligence and national strategy*, School for National Security Executive Education, Washington, D.C., National Defense University Press, viewed 02 July 2010, <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471485>.

Voris, J, Jermyn, J, Keromytis, A & Stofolso S, 2013. *Bait and snitch-Defending computer systems with decoys*, Columbia University, New York.

WEF 2014, *Insight report--Global risks 2014*, viewed 11 Feb. 2014, <http ://www.weforum.org/globalrisks2013>.

ANNEXURE D

Proceedings of the
14th European Conference on Cyber Warfare & Security

University of Hertfordshire
Hatfield, UK
2-3 July 2015

Edited by

Dr. Nasser Abouzakhar
University of Hertfordshire, UK

A conference managed by ACPI, UK

acpi

The Cyber Counterintelligence Process - a Conceptual Overview and Theoretical Proposition

Petrus Duvenage[1], Sebastian von Solms[2], Manuel Corregedor[3]
[1] Centre for Cyber Security, University of Johannesburg, South Africa
[2] Centre for Cyber Security, University of Johannesburg, South Africa
[3] Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa.
duvenage@live.co.za
basievs@uj.ac.za
200503063@student.uj.ac.za

With the ineffectiveness of the defensive cyber security toolkit against advanced threats now commonly accepted, the quest is intensifying for viable and practical alternatives. While Cyber Counterintelligence (CCI) is gaining traction as such an approach, it is still in its infancy as a field of academic enquiry. This paper aims to contribute to an area largely underexplored, namely the conceptual structuring of the CCI process.

The paper argues a proposition on the CCI process to be of critical academic and practical importance. On an academic level, such a proposition serves as a notional concept for directing and delineating further research into CCI. On a practical level, the conceptual outline of the process provides an organising template for performing CCI work in practice. On both accounts the proposition is an idealisation - where the CCI process appears to be optimally effective and where everything goes as planned.

The paper is based on the premise that CCI can only be performed effectively as part of a multi-disciplinary Counterintelligence (CI) process. Moving from this premise, a contextual overview is provided of some existing postulations on the Intelligence, CI and CCI processes. Since existing propositions do not sufficiently explain CCI, an alternative process model is presented in the form of a diagram and a narrative conceptual outline. The aim is not to describe the process in detail, but to rather present a high-level theoretical framework.

Keywords: cyber counterintelligence, cyber-counterintelligence process, offensive cybersecurity, cyber security.

1. Introduction

Key events during 2015 have affirmed the continued deterioration in cyber security and the degree to which the landscape for the foreseeable future will favour the aggressor. There are various reasons perpetuating this trend. One of these is that current security approaches, for the overwhelming part, remain stuck in antiquated processes models which are compliance-driven, defensive in posture and which emphasise technical solutions at the expense of a more holistic approach.

In an endeavour to capitalise on the market demand for alternatives, commercial cyber-security vendors are increasingly drawing on concepts, principles and approaches that have their origin, and have been proven, in state security circles. Terms and marketing slogans that have thus been gaining popularity include “threat intelligence”, “cyber intelligence” “cyber threat intelligence” and to a lesser degree “cyber counterintelligence” (Deloitte 2014*a*-b, iSight 2014, Lee 2014*a*-*e*, Firestone 2015, INSA 2011). In this regard, KPMG (2013) states: “The number of cyber threat intelligence providers is on the rise and the concept of threat intelligence is now pervasive ..... Much can be learned from law enforcement and intelligence organizations. They have long recognized that intelligence-led decision making sits at the heart of their organizational culture and operations”. More recently Kaspersky’s General Manager for Security Government Solutions, Adam Firestone (2015) warned that threat intelligence is being overemphasised at the cost of sound CCI, which draw on established CI practices. Views and interpretations sharply diverge on what the said intelligence and CI-related approaches entail, and even more so on the processes, by which they are executed. (Deloitte 2014*b*, EMC[2] 2014, Firestone 2015, INSA 2013, INSA 2014*a*-*b*, VeriSign 2012, Lee 2014*a*-*e).*

This paper holds CCI to be the most apt and viable in academically explaining and practically executing an integrated cyber security approach to confronting sophisticated threats. (The case for CCI has been argued in an earlier contribution – Duvenage & Von Solms 2013). While practised by state security structures for over twenty years, CCI remains poorly understood in the public and commercial domains. Also as a field of academic enquiry, CCI is in its infancy. While innovative research is important, it is equally imperative to first get the basics right. These basics entail the laying out and application of existing knowledge in a manner conducive to the CCI academic discourse. This paper builds on previous articles which defined various CCI concepts, positioned CCI as part of multi-disciplinary counterintelligence (CI) and explained CCI's defensive and offensive modes (Duvenage & Von Solms 2013, 2014). This paper is focussed on a further fundamental aspect, namely the CCI process. It seeks to address the problem statement: How can the counterintelligence process be structured conceptually?

To this end, the paper firstly defines concepts that are central to unpacking CCI and the CCI process. Given the prolific and confusing use of the terms 'threat intelligence' and 'cyber intelligence' when it comes to cyber security processes, care is taken to distinguish these concepts from CCI. The paper proceeds with examining the concept of a process model with a view on answering: What is a process model and why is it needed? This is followed by a brief examination of some existing process models. Existing postulations are demonstrated as describing aspects, but not the whole, of the CCI process. The paper proceeds with advancing a CCI process model which allows CCI to be executed as an integral part of the broader CI process. The paper concludes with highlighting the need for further research.

2. What is Intelligence, Counterintelligence and where does Cyber Counterintelligence fit in?

Any discussion of the CCI process firstly requires the clarification of the key concepts of 'Intelligence', CI and CCI. We can, after all not describe the process if we are not clear about what processes we are talking about. Adding to the need for such clarification, is the earlier noted prevalence in the use of "threat intelligence", "cyber intelligence" and "cyber threat intelligence" – sometimes loosely and without due consideration of their original and actual meanings of these concepts (iSight 2014, EMC^2 2014, Verisign 2012, KPMG 2013, Lee 2014*a*-*e*, INSA 2011, 2013, 2014 *a*-*b*).

Since these terms in an academic sense originate from conventional Intelligence Studies, the latter offers a useful premise. (In the interest of simplicity, and less otherwise qualified, the term Intelligence Studies is subsequently used as referring to both conventional 'Intelligence Studies' [sub-discipline of Political Science] and 'Business Intelligence' [which includes Competitive Intelligence]). While there is no consensus within Intelligence Studies on a single denotative definition, the following description conveys the meaning of intelligence in the statutory context: "Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers, the products of that process", the safeguarding of this information through counterintelligence and the carrying out of covert action (Lowenthal 2012, Godson 2001). In what can be confounding, Intelligence Studies' literature use CI juxtaposed with 'intelligence' (Sims 2009, Bodmer *et al* 2012). In this juxtaposed use, 'intelligence' is an abbreviated reference to the concept 'positive intelligence'. This double meaning underpins ambiguous uses of concepts also in the cyber field in general, and cyber processes in particular. Since the paper is primarily focused on a cyber-related process, these concepts are now distinguished in more detail. The distinction is graphically depicted in Figure 1 and then explained:

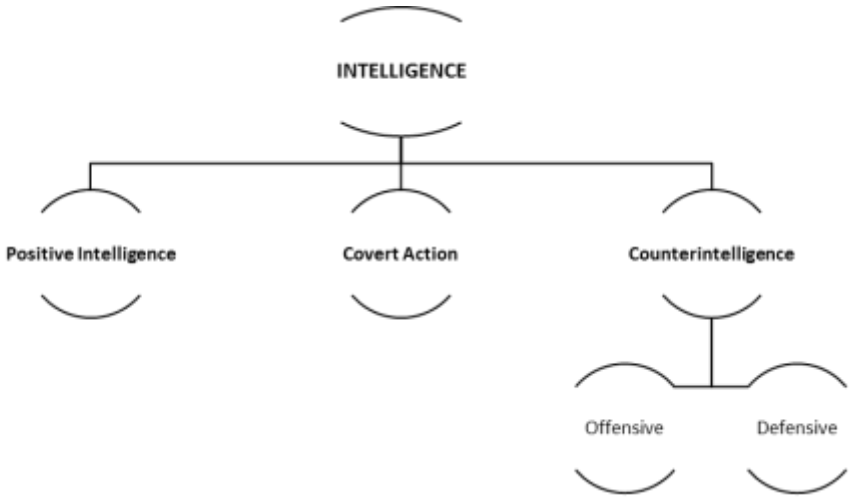


Figure 1: Intelligence and its primary disciplines (Created by the authors)

Simplified for the purpose of this paper, Intelligence is deemed to have three primary disciplines or fields, namely:

- *Positive Intelligence* that primarily aims to provide information "to facilitate one's own side achieving its ends." (Bodmer *et al* 2012). This information varies from analysed open-sources to an opponent's secrets obtained through espionage. As noted above, 'Intelligence' is frequently used interchangeably as referring to 'Positive Intelligence', with the context determining what meaning is implied (Sims 2009).
- *Covert action* which targets an adversary through the influencing of events, conditions, individuals, groups or institutions to the benefit of the client in a manner not attributable to the sponsor or offering plausible deniability. In the information sphere, covert action can take the form of propaganda, deception and disinformation (Godson, 2001).
- *Counterintelligence* is an abbreviated form for the countering of hostile intelligence activities. Counterintelligence defensively and offensively guards against adversarial intelligence (i.e. hostile positive, counterintelligence and covert action) operations (Prunkun 2012, Sims 2009).

Intelligence involves the execution of these primary disciplines in a mutually supportive manner and with functions such as collection, analysis and management performed in all three. Of these disciplines, CI is central to this paper and requires some further unpacking. CI relies on, and informs Intelligence. Similarly, CI protects and utilises some forms of covert action. CI denotes the collective of measures to identify, deter, exploit, degrade, neutralise and protect against adversarial intelligence activities deemed as detrimental or potentially detrimental to its own interests. It is directed against the actions of adversaries which include nation states, corporate entities, criminals, activists, terrorists, individuals and others. CI includes but is wider than conventional passive security. It also entails active-offensive actions to exploit and pre-emptively neutralise adversaries. CI should engage adversarial intelligence thrusts on the human (HUMINT) and technical (TECHINT) level. The cyber sphere is of course one of the technical conduits increasingly used by adversaries. It is in the latter arena which CCI functions as part a broader CI endeavour. More definitively, CCI can be described as that subset of multi-disciplinary CI aimed at detecting, deterring, preventing, degrading, exploiting and neutralising adversarial attempts to collect, alter or in any other way breach the C-I-A of valued information assets through cyber means (Duvenage & Von Solms, 2014).

The preceding definition of terms underscores the paper's contention on the loose, confusing and often incorrect use of terms such as 'threat intelligence', 'cyber intelligence', 'cyber threat intelligence' and 'cyber counterintelligence.' It is clear from the explanation 'cyber intelligence' could have two meanings. Firstly, and in its broader meaning, cyber intelligence denotes the collective of (i) positive intelligence gathered through cyber means on the environment and adversaries; (ii) cyber counterintelligence and (iii) covert action in the cyber sphere. Secondly, in a narrower connotation, 'cyber intelligence' refers to the positive cyber intelligence endeavour. Positive cyber intelligence, will involve focussing on aspects far wider than only cyber threat actors. In both its broader and narrow connotations, 'cyber intelligence' may entail the focussing, with cyber means, on actors who do not necessarily pose a cyber threat.

However, it is not uncommon to find 'cyber intelligence' and 'cyber threat intelligence' being used as referring to information collected and analysed with a view on countering mostly high-end cyber threat actors (Deloitte 2014a-*b*, EMC^2 2014, Firestone 2015, INSA 2013, INSA 2014*a*-*b*, VeriSign 2012, Lee 2014*a*-*e*.) These terms are employed to describe intelligence and actions against high-end actors who themselves execute malicious cyber following, or as part of, intelligence operations. 'Cyber intelligence' and 'cyber threat intelligence', in their popular use, furthermore denote actions aimed at detecting, deterring and neutralising these adversarial attempts. Employing the definition of CCI provided above, however, it is clear that these terms then actual deal with some aspects of CCI.

This section has delineated concepts key to the later unpacking of CCI process model. The next section reflects on the importance of a CCI process model.

3. CCI process model – what is it and why is it important?

A CCI process model, in stating the obvious, is important since CCI is of pivotal importance. Properly conceptualised and executed, CCI offers a viable approach to proactively mitigate the high-end cyber threats. Proper conceptualisation and execution in turn, has a sound process model as requisite. This is so, since CCI is an intricate process, involving a wide array of means, methods and actions; executed in various modes and manners; and for complementary ends. It is practically and academically infeasible to attempt describing the CCI process in all its detail. The strategic management and guidance of the CCI process and the demands of academic research, call for a simplification at higher level of abstraction. At this higher level, a 'bird's eye view' ought to emerge of the overarching process that coherently binds and drives the work of CCI.

As process models in general, the CCI process should be presented as a model that acts as "idealizations of processes that are more subtle and more complex in practice." (Berkowitz & Goodman, 2000). A model ought to be simultaneously congruent with reality and an idealised, simplified representation of reality. Since it is an idealisation, a model is "an aim point, of what the process should look like if everything goes as planned." (Lowenthal, 2012) Academically, it serves as a notional concept for theorising and a premise or soundboard for research. More practically, it provides a template for the organised execution of CCI functions and activities. These activities are typically clustered in various steps or stages by means of which the CCI work is conducted.

Proceeding from this demarcation of the CCI process, the next section examines some existing propositions.

4. Current propositions on, or relating to, the Cyber Counterintelligence Process

Right from the onset, the CCI process needs to be distinguished from the cyber security process. Over years, the term cyber security process has come to denote the cluster of compliance-driven activities, in which the technical aspects predominate. The implementation and adoption practices as prescribed by ISO27001 and ISO22301 were, and are still seen, as providing cyber-security processes for all types of entities. While critically important, such processes are individually and wholly insufficient.

In as far as academic and published literature is concerned, contribution on models that pertinently deal with the CCI processes are rare. One of the most authoritative works on CCI, Bodmer (et al 2012) *Reverse Deception – Organized Cyber Threat Counter- Exploitation*, for example, does not advance such a process. A notable academic work, and one of few addressing the CCI process, is that of Sigholm & Bang's (2013) entitled *Towards Offensive Cyber Counterintelligence*. With the qualification that Sigholm & Bang's (2013) work is placed within a statutory military context, their paper sets out to offer a "comprehensive process that bridges the gap between the various actors involved in CCI" (Sigholm & Bang 2013). The work subscribes to Clark's (2004) "Target-centric Intelligence Process" which was specifically developed for statutory intelligence Analysis and not the whole range of Intelligence and CI functions. Graphically Clark's model can be depicted as follows:

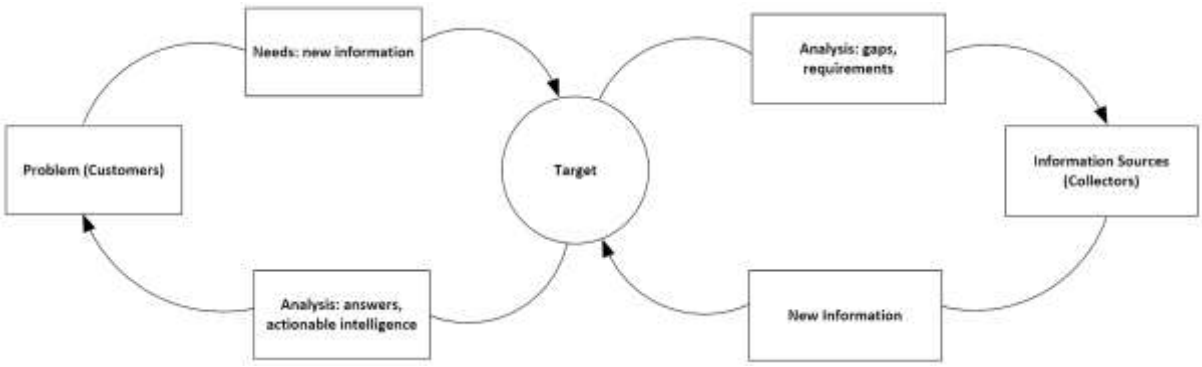


Figure 2: Target-Centric Intelligence Process (Adapted from Clark, 2004)

Drawing on this model Sigholm & Bang (2013) postulate a model for the "offensive CCI attribution process". Rather than an overarching, "comprehensive" CCI process, their proposition is on closer examination limited to one aspect of the CCI process, namely attribution and more specifically an information flow and analysis architecture to be employed for this (attribution) purpose. In their proposal, offensive CCI is neither incorporated with defensive CCI nor is it dovetailed with the broader CI process. This concept is illustrated in the following diagram provided by Sigholm & Bang (2013):

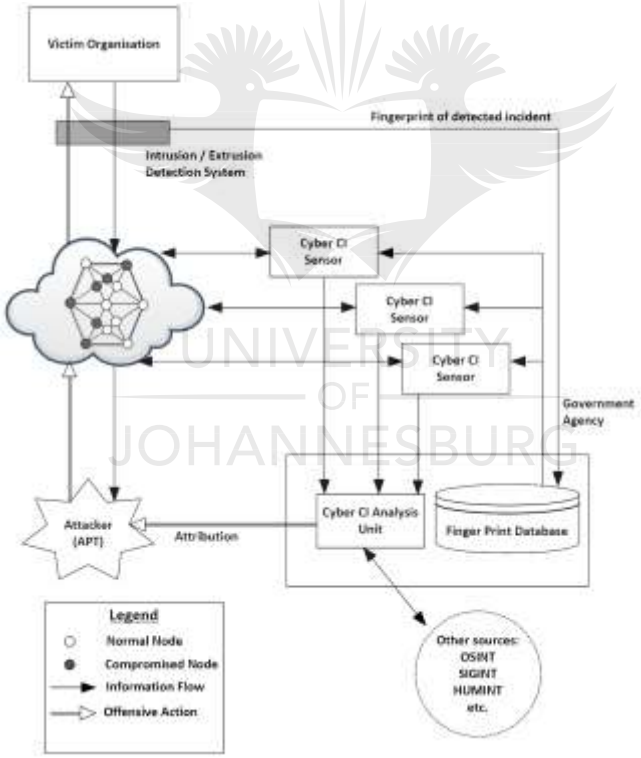


Figure 3: A layout of the offensive CCI attribution process (Adapted from Sigholm & Bang, 2013)

Literature published by cyber security entities offering CCI services do in some instances contain references to the CCI process. These vendors' contributions are cursory, aimed at expanding market share and not substantiated academic research. None of the promotional publications reviewed, purport to offer a model specifically linked to the CCI process. However, as noted earlier, the terms 'cyber intelligence' and 'cyber threat intelligence' in popular use often denote what is actually CCI. Consequently, this paper's review of the CCI process should also consider processes with these other tags. Process propositions under the tags 'cyber intelligence', and 'cyber threat intelligence' are more common. Several of these propositions strongly draw on their descriptions of the 'cyber intelligence' process on what is known in Intelligence Studies as the traditional intelligence cycle. As it has done for

more than sixty years within Intelligence Studies and statutory intelligence practice (Hulnick 2007), the traditional intelligence cycle now strongly influences thinking on Intelligence and CI processes in the cyber realm. Reduced to its essence, the intelligence cycle consists of the execution in a circular flow of the following activities: direction of the process through the clients expressing its intelligence requirements collection of information, analysis and dissemination:

Within cyber-security sphere, subscription to the intelligence cycle varies from simple adoptions at one end of the spectrum; to customised expansions at the other. Serving as an example of a simple adoption is VeriSign's (2012) *Establishing Formal Cyber Intelligence Capability (White Paper)* which states: "To successfully mount and implement an intelligence capability, it's essential to understand the intelligence lifecycle model… [the]… Traditional Intelligence Cycle comprise of Direction, Collection, Analysis and Dissemination." This description concurs exactly with the cycle as described above.

At the other end of the spectrum, KPMG (2013) advances a customised, expanded proposition as a "Basic Intelligence Operating Model" for "cyber threat intelligence". While dimensions such as "cyber intelligence strategy and budget" and "cyber intelligence sources" are added and described, the core of model – on closer analysis – still closely resembles the traditional intelligence cycle.

As would have been noted, the intelligence cycle in its simple or expanded format does not explain and / or mention CI. As is the case in Intelligence Studies, proponents of this cycle in cyber security realm may argue or imply that counterintelligence is performed throughout the cycle (cf Lee 2014 a-e, VeriSign 2012). The counterintelligence processes, this argument proceeds, mirrors and protects the intelligence cycle. In reality, these 'counterintelligence-throughout-the-cycle' and 'counterintelligence-follows-the-cycle' positions do simply not work. The intelligence cycle was originally conceived to explain positive intelligence and is not particularly good at that either. The following observation by distinguished Intelligence practitioner and scholar Arthur Hulnick (2007) is just as applicable to the cyber field: "[t]he intelligence cycle is a flawed vision, and thus poor theory. One need only ask those who have toiled in the fields of intelligence ... [C]ounterintelligence follows an entire different and unique path of its own ... It has nothing to do with the intelligence cycle. Instead there is counterintelligence methodology that is unique ... So when one looks at the pattern of counterintelligence functions, it does not look at all like the intelligence cycle."
If the intelligence cycle does not work for counterintelligence generally, it can of course not work in the cyber ream generally and for cyber counterintelligence specifically.

5. Are there alternatives in Intelligence Studies that can be applied to CCI?

Could Intelligence Studies offer a CI process that can be utilised as the basis for a CCI model? Contrary to what might have been expected, there are no current postulations offering a quick fix solution. Endeavours within Intelligence Studies over the past two decades to offer alternatives remains overwhelming directed to positive intelligence (Johnson 2007; Lowenthal 2012, Clark 2004). One of the very few propositions pertinently advanced for CI is that by Hulnick (2007). He proposes a "counterintelligence model" comprising of a five-clustered "pattern", namely "identification", "penetration", "exploitation", "interdiction" and "claim success". Summarised, Hulnick's description of the phases of the counterintelligence model are as follows:

- the identification of espionage adversaries;
- the penetration of adversarial espionage intelligence structures;
- exploitation – as referring to the collection of information (on adversaries) and the institution of measures such as deception;
- interdiction, which ensues when the "the case is turned over to law enforcement"; and,
- Public declarations by state authorities of successful counterintelligence actions.

Hulnick (2007) explicitly limits the model above to "active counterintelligence". In adding a qualification, "defensive measures in counterintelligence", are described as not fitting into "either the traditional intelligence cycle or the model just described." Within state security structures, these long-established defensive measures are commonly referred to as Operational Security (OPSEC) and comprise the following steps five steps (US 1996): Identify critical information and other assets, Analyse threats, Determine vulnerabilities, Asses risks and lastly develop and implement Countermeasures.

Effective CI requires the integrated execution of offensive/active and defensive/passive modes. They are, after all, different sides of the same coin. Are there examples of integrative proposals which combine defensive and offensive CI dimensions? While none could be found in conventional Intelligence Studies (cf Duvenage & Hough 2011), propositions exist within Business Intelligence which attempt to combine the offensive and defensive dimensions. A seminal model in this regard was forwarded by Nolan (1997). While copyright restriction prevents an inclusion of Nolan's graphical depiction in this paper, subsequent Business Intelligence propositions, convey the same thinking. The following proposal by Brouard (2004) shown in Figure 4 is an example:

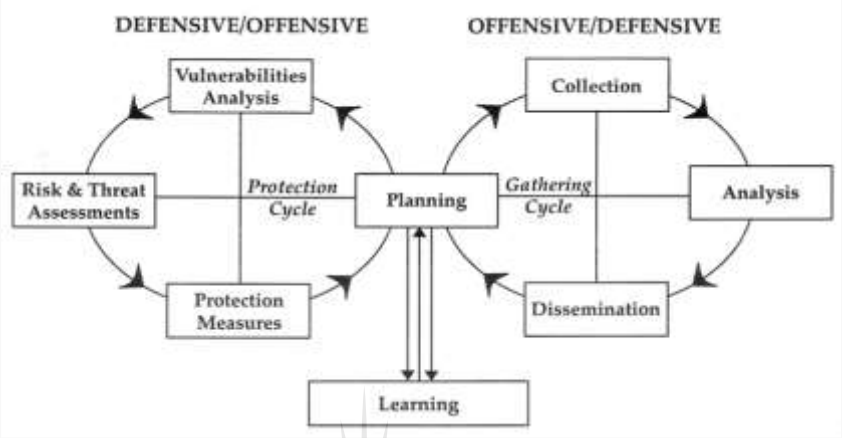


Figure 4: Intelligence Gathering and Protection Intelligence Process (Brouard, 2004)

Such models offer a useful contribution in their conceptual integration of sub-processes and the addition of a risk assessment methodology. Nonetheless, they insufficiently reflect the nature of the defensive and offensive counterintelligence thrusts as described above. They are also not granulated enough to serve either as an aiming point for practical execution or as a sounding board for further academic exploration.

6. A proposed Cyber Counterintelligence Process

This paper proposes a model that combines the respective steps of offensive and defensive CI into a single process. Within this process, the defensive and offensive sub-processes, while for a large part intertwined, also follow distinctive patterns. The paper limits itself to describing in more detail the offensive process. CCI, and to re-emphasize, is executed as part of the broader CI process. The CCI process thus looks, works and is inseparable from the CI process. Graphically, the CI process, with emphasis on CCI, is depicted in Figure 5 on the next page. This proposition builds on and contain extracts from Duvenage & Hough 2011.:

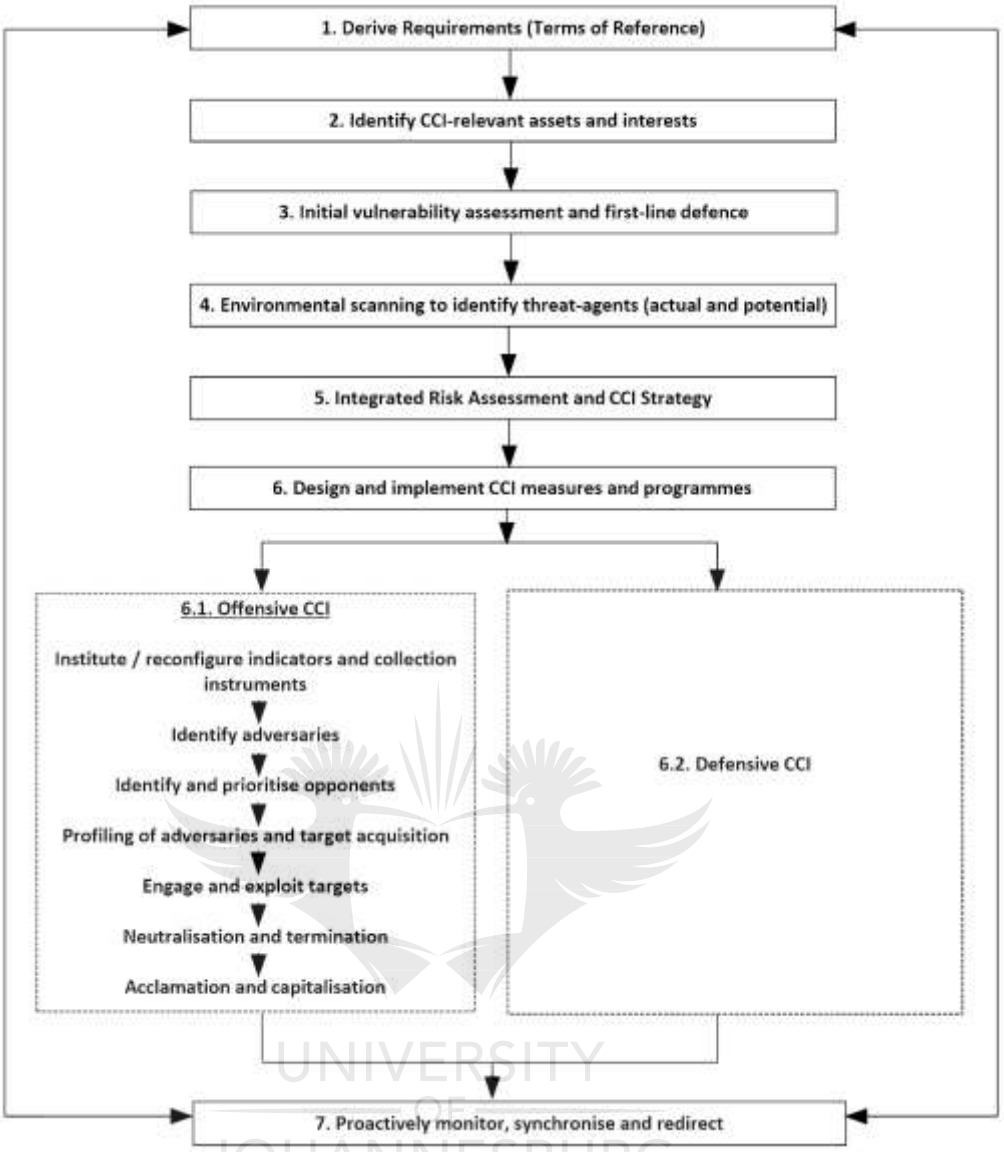


Figure 5: The Cyber Counterintelligence Process (Created by the Authors)

Although Figure 5 shows a linear sequence (i.e. neat finalisation of one step, directly followed by the execution of the subsequent steps), the CCI process is in reality multi-directional with steps being repeated and overlapping. This qualification also applies to the narrative description of the model below.

(1) Derive Requirements (Terms of Reference)

Like CI in general, CCI is not an end in itself. It serves the interest of a particular client – be it a government or business. The client expects from its CI apparatus to not only safeguard its vital interests and objectives, but to actively advance these. Ideally, CCI (as part of the broader CI process) would commence with the client clearly expressing its expectations. These would include: what cyber assets should be protected and what CCI should do to pro-actively promote government or company interests. This is very rarely the case. CI and CCI requirements are mostly derived and not received. They are derived through a meticulous appraisal of the client's objectives, intentions and strategy. Preferably these should be contained in Terms of Reference (ToR) endorsed by the client and within the parameters set by legal jurisdictions.

(2) Identify Assets to be Protected and Interests to be Advanced

Resources are finite and CCI can only execute its signature role to defend and neutralise in a highly prioritised and selective manner. The right place to start is to ascertain what assets and interests in the information-cyber sphere are worthy of protection. In the case of nation states (or other sizable role-

players) these info-cyber assets and interests – identified on the basis of the ToR - are threefold. Firstly, assets the state possesses which is central for survival and prosperity. Such assets include critical bodies of information, systems and infrastructure. Secondly, assets the state aspires to procure through cyber means (such as the secrets of adversaries). Thirdly, critical interests refer to the conditions the state seeks to realise (for example, the gaining of a competitive edge through obtaining adversarial secrets, adding additional layers to its defences or offensively undermining the C-I-A of adversarial systems).

(3) Initial vulnerability assessment and first-line defence

Although there are exceptions, the CI doctrine requires offensive action to be preceded by solid defence. Applied to CCI, the identification of real and aspirational assets and interests described above, is therefore followed by identifying the vulnerabilities in defensive and cyber-security measures which protect these assets and interest. This process would typically result in remedial action in relation to cyber, information, physical and personal security. It thus also involves CI specialisation fields other than CCI. This sub-process is again performed, but more exhaustively, as part of step 6.2. Care should be taken not to summarily close all 'holes' in the cyber 'fences'. Some of these could be exploited for offensive purposes later on in Step 6.

(4) Environmental scanning to identify threat-agents (actual & potential)

The assessment performed in the previous step mostly considered internal weaknesses and vulnerabilities. Effective CI needs to safeguard against and engage external threats. While opponents (competitors and adversaries) are common threat actors, risks can also be posed by technological and socio-political developments. While all of these are not a CI and CCI concern, they are considered for inferring actual and potential threats agents (of CI relevance). A common pitfall is to identify threat agents mainly on the basis of actors known to be active, adversarial and well-capacitated. The result is a self-feeding, atrophic CCI process with risks posed by previously unknown threat actors going undetected. The importance of innovative environmental scanning, which aims to identify potential threat agents hardly be overemphasised.

(5) Integrated Risk Assessment and Strategy

Considering the external and internal threats as well as vulnerabilities and weaknesses identified in preceding steps, the CCI process proceeds to perform an integrated risk assessment. The risk assessment identifies which CCI measures are obsolete, which require modification, and in which areas they are lacking. Decisions taken on CCI are formulated as part of a broader CI strategy which combines defensive and offensive dimensions. A balance needs to be maintained between, to paraphrase Nolan (1997), defensive CI tasks to 'close holes in the fence', and offensive CI that seeks to exploit the offensive opportunities that vulnerabilities offer.

(6) Design and implement CCI measures and programmes

While offensive and defensive measures are designed and implemented in synergy each sub-process has a unique mission and thus pattern of execution. This paper limits itself to outlining the offensive pattern which consists of the following six steps:

(6.1.1) Institute/reconfigure indicators and collection instruments

Since espionage is both a precursor and end-aim of sophisticated cyber breaches , the offensive sub-process commences with instituting and/or reconfiguring (a) indicators of adversarial cyber espionage and (b) own collection instruments. Whatever form these instruments take (honeynets, tarpits, footholds in on-line communities and sites, etc.), they will be developed and are constantly fine-tuned around most prized assets. In steps 6.1.3 and 6.1.4 these instruments will be further optimised to best collect on and then engage targets.

(6.1.2) Identify and prioritise intelligence opponents

In addition to information obtained through the preceding step, CCI will draw on the broader, all-source CI picture to identify opponents who are and potentially are targeting their own entities though intelligence actions such of espionage, covert action, and so on. Even the well-resourced entities cannot offensively focus on all known and suspected opponents. Consequently, only prioritized opponents are elevated to actual/potential adversaries and pursued through further offensive action.

(6.1.3) In-depth 'profiling' of adversaries to arrive at targets

These offensive actions firstly entail focused information collection on, and subsequent in-depth profiling of adversaries. The focused collection of information is high-risk and high cost measures and

could include cyber espionage. A crucial CCI collection requirement is to ascertain the instrumentalities and proxies adversaries use for intelligence activities. To this end, information procured through other conduits such as HUMINT and other TECHINT are also used. Depending on various factors some of these adversaries, their proxies or campaigns are not suited for offensive exploitation and as such will be channelled to defensive CCI.

(6.1.4) Engagement and exploitation of targets

As is apparent from the above, the acquisition of targets (prioritised adversaries and their proxies) for offensive action is an exhaustive process. In certain respects the acquisition of targets is the most complex part of CCI work. To adopt a Clark (2004) target-centric-type view at the start of the process, would thus clearly be a gross over-simplification which skips over critical segments of the CCI methodology. The engagement and exploitation of targets are at offensive CCI's core. These exploitations can take a myriad of forms and include escalated (more aggressive) collection, deception, manipulation, disinformation as well as the disruption of hostile intelligence activities. The ideal aim of CCI is the degrading and control of the adversary through their own cyber actions. The following observation by Codevilla (1992) rings true also in respect of CCI: "Action against the enemy through the enemy's own intelligence is the very consummation of CI." Usually this is best achieved through combining CCI within other forms of offensive CI. Deception through honeynets and sock puppets could, for example, be supplemented through disinformation fed through a human double agent.

(6.1.5) Neutralisation and termination

While the targets are to a certain level neutralised through exploitation, offensive CCI operations would typically have a 'neutralisation and termination' phase at the end of their 'life-cycle'. Termination can either be opted for (i.e. at own initiative at a pre-determined time) or necessitated by circumstances (such as indications that an operation has been compromised). Whatever the case, termination should be planned for in advance with two purposes. Firstly, delivering the final neutralisation 'blow' to the adversarial campaigns being engaged. Secondly, if executed skilfully, providing the 'seeds' for a subsequent 'generation' of CCI operations.

(6.1.6) Acclamation, reflection and identification of further opportunities

As with CI generally, CCI success ought to be followed by acclamation. There are two kinds of acclamations: Firstly, public acclamation in which aspects of the successful countering of hostile cyber intelligence activities would be cited. In the case of governments, such claiming of success is vital in justifying in the public eye the billions spent on Intelligence, CI and CCI. Moreover, public acclamation can be part of degrading an adversary. Secondly acclamation can be limited on the need-to-know principle. Sometimes entities should "try hard to keep successes secret so that they might be repeated. An oft-quoted CIA saying is, 'The secret of our success is the secret of our success.' "(Hulnick 2007). Whatever acclamation opted for, concluded CCI operations are assessed for lessons learned and to identify opportunities for further exploitation.

(7) Monitor, synchronise and redirect

Although indicated as a separate step in the interest of simplicity, CCI is continuously monitored and synchronised and redirected in accordance with the broader CI and Intelligence effort. The latter in turn, ought to be dovetailed with an entity's Objectives and Strategy. Intelligence and CI of any kind are instruments and not ends in themselves. The intelligence and insights gained through this endeavour influence Objectives, Strategy and thus eventually the ToR of the on-going Intelligence process of which CCI is a part of.

7. Conclusion

This paper moved from the premise that the nature of the current and future cyber threatscape necessitates an integrated cyber security approach with CCI at its core. Sophisticated threats, it was argued, have intelligence actions (such as espionage) as its essential feature. The paper explained the importance of process models and found existing propositions to be insufficient in explaining the CCI. Nonetheless, the discourse on the intelligence and CI process generally, did provide elements which were useful for the construction of a CCI process model. The paper proceeded with postulating a theoretical framework for the CCI process. This postulation does not purport to offer radically new insights. It is, instead, a tentative proposal intended to stimulate future debate and theory constructions.

References

Bodmer, S. A. *et al* (2012) *Hacking Back: Offensive Cyber Counterintelligence*, McGraw-Hill, New York.

Berkowitz, B. D. & Goodman, A. E. (2000) *Best Truth: Intelligence in the Information Age*. New Haven: Yale University Press.

Brouard, F. (2004) "Business intelligence for Canadian corporations after September 11." *Journal of Competitive Intelligence and Management*, Vol 2, No 1.

Clarke, R. M. (2004) *Intelligence Analysis: A Target-centric Approach*, CQ Press, Washington D.C.

Codevilla, A. (1992) Informing *statecraft – intelligence for a new century*. New York. The Free Press.

Deloitte (2014*a*) "Cyber threat Intelligence: Moving to an Intelligence-driven cybersecurity model'" *Insight* , CIO edition. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/

Deloitte (2014*b*) *Transforming cybersecurity New approaches for an evolving threat landscape*. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/.../ 021114.pdf

Duvenage, P.C. & Hough, M. (2011) "The Conceptual Structuring of the Intelligence and the Counterintelligence Processes", *Strategic Review for Southern Africa*, University of Pretoria, Pretoria.

Duvenage, P. C. & von Solms. S.H. (2014) "Cyber Counterintelligence: Back to the Future", *Journal of Information Warfare*, Vol 13, Issue 4 .

Duvenage, P. C. & von Solms. S.H. (2013) "The Case for Cyber Counterintelligence", paper read at *5th International Workshop on ICT Uses In Warfare and the Safeguarding of Peace (IWSP'13)*, Pretoria, Soutyh Africa.

EMC^2 (2014) *Intelligence Driven Threat Detection and Response, (White paper).* Retrieved from http://southafrica.emc.com/collateral/white-paper/h1304-intelligence-driven-threat-detection-response-wp.pdf.

Firestone, A. (2015) "Shifting Paradigms: The Case for Cyber Counter-Intelligence", *InformationWeek*. Retrieved from http://www.darkreading.com/operations/shifting-paradigms-the-case-for-cyber-counter-intelligence/

Godson, R. (2001) *Dirty tricks or trump cards?* Transaction Publishers, New Brunswick.

Hulnick, A. S. (2007) "What's Wrong with the Intelligence Cycle", in Johnson, L K (ed), *Strategic Intelligence (Vol 4) — The Intelligence Cycle.* Praeger Securities International, Westport.

INSA Intelligence and National Security Alliance (2014*a) Operational Threat Intelligence.* Retrieved on 24 January 2015 from http://www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx

INSA (2014*b) Strategic Cyber Intelligence*, Retrieved on 24 January 2015 from http://www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx

INSA (2013) *Operational Levels of Cyber Intelligence*. Retrieved on 07 October 2014 from http://issuu.com/insalliance/docs/ insa_wp_cyberintelligence_pages_hir/16?e= 6126110/4859250

INSA (2011) *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*. Retrieved on 06 October 2014 from http://www.insaonline.org/i/d/a/Resources/Cyber_ Intelligence.aspx

iSightpartners. (2014) *What is Cyber Threat Intelligence?.* Retrieved from *http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief 1.pdf*

KPMG (2013) *Cyber threat intelligence: lessons from law enforcement*. Retrieved from http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-threat-intelligence-final3.pdf

Lee, R. M. (2014*a*), "An Introduction to Cyber Intelligence", *Tripwire*, blog series, Part 1, Retrieved 04/01/15 from http://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/

Lee, R. M. (2014*b*) "Developing Your Cyber Intelligence Analyst Skills", *Tripwire* , blog series, Part 2. Retrieved on 04/01/15 from http://www.tripwire.com/.../developing-cyber-intelligence-analyst-skills/

Lee, R. M. (2014*c*), "Cyber Intelligence Collection Operations", *Tripwire*, blog series, part 3. Retrieved on 04/01/15 from http://www.tripwire.com/.../cyber-intelligence-collection-operations/

Lee, R. M. (2014*d*) "Cyber Counterintelligence: Theory to Practice", *Tripwire* , blog series, part 4. Retrieved on 04/01/15 from http://www.tripwire.com/.../cyber-counterintelligence-from-theory-to-practice/

Lee, R. M. (2014*e)* "Cyber Threat Intelligence", *Tripwire*, blog series, part 5. Retrieved on 04/01/15 from http://www.tripwire.com/.../state-of-security/security-data-protection/cyber-threat-intelligence/

Lowenthal, M.M. (2012) *Intelligence: from Secrets to Policy*, fifth edition, CQ Press, California.

Prunckun, H. (2012) *Counterintelligence: Theory and Practice*. Plymouth, Rowman & Little Publishers.

Sigholm, J & Bang, M "Towards Offensive Cyber Counterintelligence - Adopting a Target-Centric View on Advanced Persistent Threats", paper read at the 2013 European Intelligence and Security Informatics Conference

Sims, J. E. (2009) "Twenty-first-Century Counterintelligence" in Sims, J. E. and Gerber, B. (eds.) *Vaults, Mirrors and Masks – Rediscovering U.S. Counterintelligence*. Georgetown University Press, Washington (D.C.)

United States of America, *Operations Security Intelligence Threat Handbook*, Interagency Operational Security Support Staff, 1996. Retrieved on 02 May 2007 from http:www.fas.org/irp/nsa/ioss/threat96/part03.htm

VeriSign (2012) *Establishing a Formal Cyber Intelligence Capability,* White Paper, retrieved on November 17, 2014 from https://www.verisigninc.com/assets/whitepaper-idefense-cyber-intel.pdf.

ANNEXURE E

Universität der Bundeswehr München

Research Center Cyber Defence

Universität der Bundeswehr München

Research Center Cyber Defence

Proceedings of the
15th European Conference on Cyber Warfare and Security

Bundeswehr University
Munich, Germany
7-8 July 2016

Edited by
Gabi Rodosek and Robert Koch

A conference managed by ACPI, UK

acpi

Review Process
Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy
ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:
http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academic-conferences-and-publishing-international-limited/

Conference Proceedings
The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

The Electronic version of the Conference Proceedings is available to download from DROPBOX. (http://tinyurl.com/ECCWS2016) Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.

The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

Print version ISSN: 2048-8610
Print version ISBN: 978-1-910810-93-4
E-Book ISSN: 2048-8602
E-Book ISBN: 978-1-910810-96-5

Published by Academic Conferences and Publishing International Limited
Reading, UK. 44-118-972-4148. www.academic-publishing.org

Conceptualising Cyber Counterintelligence – Two Tentative Building Blocks

Petrus Duvenage[1], Victor Jaquire[2], Sebastian von Solms[1]
[1] Centre for Cyber Security, University of Johannesburg, South Africa
[2] Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa.

duvenage@live.co.za ,jaquire@gmail.com, basievs@uj.ac.za

Several escalating trends are affirming the centrality of Cyber Counterintelligence (CCI) in effectively addressing advanced cyber threats of today and tomorrow. Yet, in comparison with the burgeoning academic and commercial literature on the related field of Cyber Threat Intelligence (CTI), CCI remains vastly unexplored. Outside the circles of governments' security apparatus, some large corporates and niche vendors that offer such specialised services, CCI is still obscure. While interest is gradually growing in CCI, this academic discipline is very young and largely uncharted. Leveraging off previous research by the aforementioned authors, this paper advances two further building blocks to contribute towards constructing this emerging discipline.

Building block 1 comprises a distinction between CCI and CTI. Such a distinction is necessary for clarity and has the advantages of allowing CCI to benefit from the extensive research work done in the CTI field.

Building block 2 consists of a multi-layered framework that explicates the different levels on which CCI functions, namely the strategic, operational and tactical functional levels. This framework progresses building block 1. While these functional levels have been described extensively in CTI literature, no such CCI-specific application could be found in literature within the public domain. Since it expounds CCI on the various levels that it functions, the framework contributes to a more nuanced academic conceptualisation of this discipline of CCI. On a practical level, the framework could serve as a notional guide for performing actual CCI work more effectively. The article concludes by reiterating the importance of CCI in addressing advanced threats and suggesting areas for further research.

Keywords: cyber counterintelligence, cyber threat intelligence, offensive cybersecurity, cyber counterintelligence levels, cyber counterintelligence maturity.

1. Introduction

In what has become a recurring theme in recent years, industry threat reports for 2015 to 2016 highlighted the escalating damage caused and threats posed by cyber actors of increasing sophistication (Kaspersky 2015, McAfee 2015, Crowdstrike 2016). This trend is accelerating despite a continuing increase in global spend on cyber security. In recent years, vendors have been pushing particularly Cyber Threat Intelligence (CTI) as a critical part of the 'solution' and it has evolved to one of the fastest growing cyber security sectors. The $1, 02 billion global spend on CTI in 2015, for example, represents a 129% increase compared to 2011 (Statista 2016, Info-security Magazine 2015). Further attesting to threat intelligence's rising prominence is the escalation in Google search results from a mere 18 700 in 2011 to 381 000 in February 2016 (Chismon & Ruks 2015, Google 2016).

As matters currently stand, the CTI market buzz and spending of resources have not by any measure translated in a corresponding mitigation of advanced threats – nor is it likely to do so in the near future. There are various reasons for this rather gloomy prognosis of which two will be highlighted in this paper.

The first reason is that a significant portion of products and services and that are marketed as CTI is not intelligence at all. They are mere re-labelled data feeds or anti-virus packages. Of course products of this nature have a role, but they are wholly insufficient against higher-end threats. It can rightly be argued that sound CTI as part of an effective cyber-security approach would be effective in addressing advanced threats. This is indeed the case, but only partially. CTI employed as part of an effective cyber-security approach will address a substantial portion of cyber threats. It will, however, not be effective against those high-end threats that should top our concern. For CTI to be effective against these threats, it needs to be embedded in counterintelligence (CI).

The second reason for CTI not delivering on expectations is that CI is simply not being embraced. Organisations with significant cyber assets are too slow to realise that we are faced with CI challenges rather than cyber security problems. Perhaps, we are still too attached to outdated, neat tables linking specific cyber actor types to certain methods and aims. In reality, the distinction between what was conventionally labelled as state-sponsored Advanced Persistent Threats (APTs) and the actions of other actors is blurring fast. In its 2015 Global Threat Report, Crowdstrike (2016) states, for example, that "the primary motivation behind global cyber activity has now shifted from disparate activities carried out by individuals, groups and criminal gangs pursuing short-term financial gain, to skilled adversaries driven by broader agendas." The cyber criminals' aim, asserts PwC (2016), currently "goes beyond targeting financial information to include a company's 'crown jewels' – customer data and intellectual property information, the loss of which can bring down an entire business." Various types of threat actors can and do cooperate (INSA 2011). The tradecraft, activities and even aims of various classes of threat actors in cyber space are often difficult to separate and reflect high skill levels in intelligence and counterintelligence (Moyo 2015). For state and non-state actors (such as criminal groups, some corporate entities) multi-vectored espionage (e.g. human and technical means) has become a precursor to extensive breaches. The addressing of such threats is CCI's signature role.

While CI/CCI awareness within board rooms appears to be growing, these concepts are far less known than CTI (cf. SpearTip 2015, The Economist 2015). Moreover, the symbiotic relationship that should exist between CCI and CTI is seldom addressed. Therefore academia has a crucial role in conceptualising CCI clearly. This paper proposes two further building blocks that could aid in conceptualising this discipline. Firstly, CCI is distinguished from CTI and the relationship between these constructs examined. Secondly, a multi-layered framework is submitted to explicate the different levels on which CCI functions. Notionally and practically, this multi-levelled examination provides clarity on what CCI is, what it does and what its relation with CTI is.

It needs to be emphasised that this paper builds on previous articles that defined various CCI concepts, positioned CCI as part of multi-disciplinary CI, detailed CCI's defensive-offensive modes and advanced a process model (Duvenage & von Solms 2015; Duvenage, von Solms & Corregedor 2015). While some aspects of previous work are concisely recapitulated (per Section 2.2), the latter is highly selective and could not address all aspect necessary for context.

The foregoing introduction highlighted the importance of CCI in addressing current and future cyber threats. Subsequently, the need to further conceptualise CCI was underlined. The next section delineates CCI and CTI by offering definitions and discussing the relationship between the constructs.

2. Conceptual clarification – what are 'Threat Intelligence' and 'Cyber Counterintelligence'

As suggested above, CTI and CCI are interrelated yet distinct concepts. Delineating these two constructs is important, since each has a unique and complementary role in ensuring cyber security. Moreover, a clear differentiation would enable CCI to draw on extensive CTI literature in a manner that is academically credible and responsible.

2.1 Defining 'Cyber Threat Intelligence'

The rapid market growth in the market of CTI products and services has been accompanied by a proliferation in terms and definitions. "Threat intelligence", "cyber intelligence", "cyber threat intelligence" are sometimes used interchangeably and sometimes with different connotations (Deloitte 2014, Schoeman 2015, EMC^2 2014, INSA 2013, INSA 2014*a*-*b*, Lee 2014*a*-*b*.). A dissection of all these terms will distract from the paper's main focus and be more confusing than helpful. In the interest of simplicity CTI is henceforth employed in the paper as the umbrella term. Schoeman (2015) rightly states that CTI has evolved in a "catchall term for a vast array of different technologies, methodologies and ideas." Products and services sold under this banner can vary extensively in scope, usability, aims and contents (Chismon & Ruks, 2015). At the one end of the spectrum CTI can be just anti-virus signatures at a much higher cost; while at the other end, it can mean an overarching approach central to an organisation's strategy (Schoeman 2015, Riley 2015).

The term 'threat intelligence' has its roots in the concept 'intelligence' as used with state security apparatus and Intelligence Studies. Depending on context, 'Intelligence' can have several meanings

within Intelligence Studies. Intelligence can denote the overarching discipline that comprises Positive Intelligence, Counterintelligence and Covert Action. Sometimes Intelligence is often employed as a shortened reference to Positive Intelligence. The term Intelligence could furthermore refer to the outcome of a process that delivers actionable, analysed information. These meanings and applications thereof in the cyber realm were explored in an earlier article (Duvenage, von Solms & Corregedor, 2015). Suffice it to note here that 'intelligence' used in 'cyber threat intelligence' – and as henceforth applied in this paper – means actionable, assessed information on a cyber-related hazard to an entity. This is in line with Gartner's defining of threat intelligence as: "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard" (Schoeman 2015). Deriving intelligence from information and data requires analysis performed by humans. Tools and data feeds cannot by themselves provide threat intelligence (Schoeman 2015). In this regard Lee (2014*a*) states "Intelligence of any type requires analysis. Analysis is performed by humans. Automation, analytics and various tools can drastically increase the effectiveness of analysts but there must always be analysts involved in the process." In summary it can thus be said that data is processed and refined to produce information. Information is in turn analysed and presented in a format that is actionable and constitutes intelligence. In the case of CTI, this is intelligence produced on cyber-related hazards.

Ideally CTI should provide intelligence on a full spectrum of adversarial action in the cyber sphere from decision to execution. INSA (2013) provides the following breakdown of these actions and what cyber threat analysis should consider:

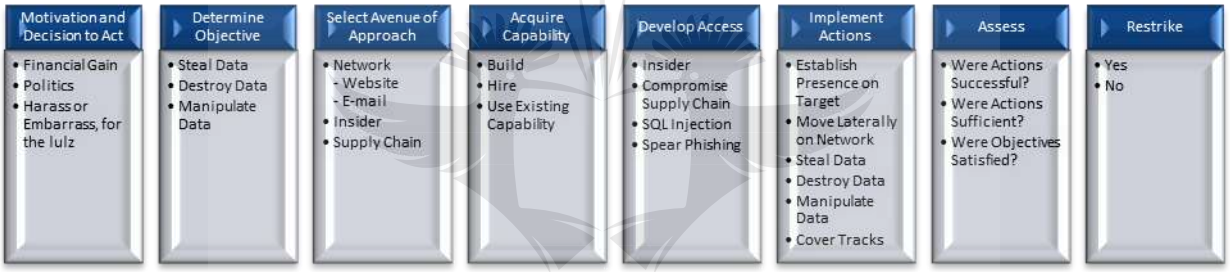


Figure 1: Adversarial Pathway to an Attack as aid for Cyber Intelligence Analysts (INSA 2013).

CTI is thus not a "collection discipline" but more of an "analytical discipline" that informs "decision makers on issues pertaining to all levels in the cyber domain", namely the strategic, operational and tactical (Mattern et al 2014). On a strategic level, CTI should identify the intent, capability and opportunity that actual and potential malicious actors could have (Lee 2014*a*). On a tactical level, CTI identifies network threats and informs responses. Bridging the mostly non-technical strategic and narrow technical/tactical layers, the operational level is focussed on an organisation's immediate operating environment (INSA, 2014*a*).

Moving from the conceptualisation of CTI in the preceding paragraphs, the notion of CCI and its relation with CTI are now examined.

2.2 Delineating Cyber Counterintelligence and its relation with Cyber Threat Intelligence

What then is CCI, how does it differ from CTI and what is the relation between these fields? As will be shown in this subsection, CCI's focus is paradoxically narrower and broader than that of CTI. CCI is narrower in that its external dimension is directed against a very specific category of "cyber hazards", namely that of hostile intelligence actions playing out in the cyber sphere. However, CCI is also broader than CTI in several respects. CCI is for one not limited to the producing and disseminating of intelligence. It also engages internal and external threats through a wide array of offensive and defensive measures. These measures are executed in synergy in accordance with the principles of traditional, multi-disciplinary CI.

2.2.1 Demarcating Counterintelligence

Therefore, CCI and its relation with CTI, can only be understood and definitively defined within the context of CI generally. CI has been discussed in some detail in earlier contributions (Duvenage & von

Solms 2015; Duvenage, von Solms & Corregedor 2015). Since familiarity with the concept CI is essential for further unpacking of CCI and for contextualising the CCI framework, a brief recapitulation is provided here.

As suggested by its composite terms 'counter' and 'intelligence', counterintelligence is essentially about the countering of hostile intelligence actions. Of these hostile intelligence actions, espionage (i.e. secret intelligence gathering) is perhaps the best known example. In addition to espionage, hostile intelligence activities also can include covert action (e.g. non-attributable influencing and deception). These hostile intelligence actions target valuable bodies of information as well as the people, processes, technologies and repositories wherein it resides. Hostile intelligence actors typically execute their actions through a combination of human ('spies') and technical means. The exploitation of the cyber sphere to realise intelligence ends is part of such technical means.

The CI mission is to safeguard, but also to advance organisational strategy and assets actively. In order to execute its mission, CI has three main thrusts namely an offensive focus, a defensive focus and an intelligence function. These three dimensions constitute the CI trident. In execution of these three dimensions, CI relies on an extensive array of means, measures and methods. In traditional CI, this ranges from defensive information security measures to the offensive running of a mole or double agent. These thrusts and their relation with means, measures and methods are explained in more detail as part of the discussion on CCI.

To summarise CI can be defined as the activities conducted to "identify, deter, exploit, degrade, neutralise and protect against adversarial intelligence activities deemed as detrimental or potentially detrimental to the own interests" (Duvenage, von Solms, Corregedor 2015). Effective CI takes on, and guard against, hostile intelligence on a human (HUMINT) and technical (TECHINT) level. This technical level includes the cyber sphere as one of its conduits.

2.2.2 Defining Cyber Counterintelligence and its relation with Cyber Threat Intelligence

Building on the preceding outline, CCI can be "described as that subset of multi-disciplinary CI aimed at detecting, deterring, preventing, degrading, exploiting and neutralisation of adversarial attempts to collect, alter or in any other way breach the C-I-A [confidentiality, integrity and availability] of valued information assets through cyber means" (Duvenage & von Solms 2015; Duvenage, von Solms, Corregedor 2015). As is clear from this definition, CCI shares CI's defensive and offensive missions (Bardin 2011). Defensive CCI seeks to deny an opponent the access it seeks, to guard the organisation against insider threats and vulnerability (Bodmer et al 2012). Offensive CCI's signature role is engaging and exploiting adversarial cyber actions to own advantage. It aims to neutralise a competitor's intelligence efforts through measures ranging from deception and manipulation to the degrading of adversarial cyber intelligence activities and systems (Farchi 2012, Lee 2014*b*). This exploitation can take the form of deception, disinformation and degrading. The ultimate aim of offensive CCI should be the control and exploitation of an adversary through the manipulation of its cyber intelligence action.

Effective defensive and offensive CCI cannot be executed blindly but is guided by intelligence. Similar to CTI, analysis is necessary to generate intelligence from information and data collected. Since CCI is about the outmanoeuvring of intelligence adversaries, high-quality analysis is imperative. In this regard Godson (2001) states: "Perhaps the queen of the counterintelligence chessboard is analysis – both offensive and defensive." CCI requires this high-grade intelligence on own cyber-relevant vulnerabilities (weaknesses of people, processes, facilities and technologies) actual and potential adversaries as well as on a strategic level, the macro-environment.

CCI executes it offensive-offensive missions and the collection of data and information through a wide array of measures (Bardin 2011). It must be emphasised that care should be taken not to categorise a CCI measure or methods rigidly as defensive or offensive. In numerous instances a measure can be of service to both the defensive and offensive missions. In addition, several of the offensive-defensive measures collect data or information of relevance to the CCI intelligence mission. These measures and the multi-purposes they serve are shown in the taxonomy provided in Table 1 (next page).

Table 1: A taxonomy of CCI Means, Methods and Measures (updated and adapted from Duvenage & von Solms, 2015)

<table>
<tr><th colspan="3">Defensive Mode</th></tr>
<tr><td colspan="3">Passive ⟷ Active</td></tr>
<tr><td>Deny</td><td>Detect</td><td>Collect</td></tr>
<tr><td>Physical Defensive</td><td>Personnel/User Defensive</td><td>System Defensive</td></tr>
<tr><td>Protects against:
• Unauthorised access to facilities and systems
• In loco theft of data, hardware
• Introduction of malware through physical access to systems
• Unauthorised altering or destruction of data
• Physical destruction or access denial
• Unauthorised reading (acoustic, visual, radiation, analogue, signals)
• While not conventionally seen as a Physical Defence, supply-chain management has a physical defensive function. It is also part of System Defences as an enabler.</td><td>Consists of aspects such as:
• IT and user personnel vetting, re-vetting, confidentiality agreements and monitoring
• Personnel security measures, BYOD user parameters or exclusions
• User programmes in cyber security that cover policy and procedures for the handling of security-related incidents, malfunctions and recovery.
• Overlapping with system defences, the use of software decoys and traps to mitigate the insider threat
• Investigations focussed on cyber security incidents involving personnel. Could also include digital forensic investigations.</td><td>Comprises a combination of:
• Hardware and software such as:
✓Network perimeter-based security (filters, certain firewalls, IDS and IPS etc.) Malware scanners.
✓Integrated automated systems/tools (that collect and evaluate information about devices connected to a network, activities thereon – inclusive of intrusions). Examples of such tools, discussed further on in the table, are decoys, honeypots and behavioural analyses toolsets.
✓Overlapping with the latter, depending on its configuration, a honeynet can be defensive or offensive in type/mode. The term fish bowling denotes the defensive configuration.
• Processes (such as supply-chain management are also in part system defences).
• Vulnerability assessments, penetration testing and verification testing (on products, systems, software and secure code).
• Incident and threat monitoring, identification, investigation and response. A CERT is per definition defensive – although it might contain offensive elements in its responsive action.
• Port level security and BYOD regulation in as far as network interfacing is concerned (Also part of Personnel Defences).</td></tr>
<tr><td></td><td colspan="2">• Commercial Cyber Threat Intelligence products, services and platforms.</td></tr>
<tr><td></td><td colspan="2">• The use of software decoys to mitigate the insider threat is an overlap between personnel and system defensive measures. They are mostly active CCI means.</td></tr>
<tr><td></td><td>• Investigations focussed on internal cyber security incidents involving personnel. May include digital forensic investigations.</td><td>• Investigations of external cyber intrusions could be part passive and part active system defence.</td></tr>
<tr><th colspan="3">Offensive Mode</th></tr>
<tr><td colspan="3">Passive ⟷ Active</td></tr>
<tr><td>Collect</td><td>Disrupt</td><td>Exploit</td><td>Destroy</td></tr>
<tr><td colspan="2">• Collection of information on and the monitoring/surveillance of the cyber sphere to detect cyber adversaries and their exploitation of the cyber sphere in a manner that is not own-network restricted – (i.e. requires more than deployment of systems described under defensive mode). Could, depending on configuration also include IDS/IPS, honey-client applications (as opposed to host-based honeypots), luring and some forms of data mining.
• The recruitment and handling of virtual agents on underground forums (under true or false flag) that can serve the purpose of enticement, collection and/or exploitation. (Under certain circumstances virtual agents can also develop into HUMINT assets).</td><td>Measures taken to exploit and neutralise adversaries activities in the cyber sphere:
• System and honeynet configured offensively with the aim of enticing, exploiting and deceiving adversaries. False information is displayed to adversarial reconnaissance tools, network scanners and listeners, etc. This has as one of its aims to lead adversaries in the direction of your own preference.
• Utilisation of virtual agents for offensive purposes.</td><td rowspan="2">Cyber warfare, in the full extent of the term, is typically excluded from the mandate of civilian intelligence communities. A cyber warfare capability should be flexible and allow utilisation without, or in conjunction with, kinetic war.

Nevertheless, a top class civilian CCI outfit will need to have the authority and capacity to very selectively conduct operations that have cyber warfare characteristics, utilising cyberwarfare- related techniques. Such cyber CCI operations will share characteristics with covert action. (Covert action aims to influence role-players, conditions and events without revealing the sponsors identity.)

Within business, the use of offensive measures will be determined by the legislative and regulatory framework within which the entity operates.</td></tr>
<tr><td colspan="3">• Cyberespionage on adversaries. Distinguishable from own-system collection (IPS, IDS, honeynets etc) on the basis that adversarial networks are targeted actively and exploited in accordance with strategic and operational objectives.</td></tr>
</table>

The preceding discussion and table show that CCI, in contrast to CTI, is not only about the delivery of intelligence products. It includes active and passive measures instituted as part of an integrated approach. Moreover, the intelligence that CCI generates covers a scope significantly wider than the actor-centric intelligence associated with CTI. From both these perspectives, CTI can thus be posited as a constituent part of CCI (cf Lee 2014*b*). Figure 2 – that should be read with the qualification on the term 'intelligence in subsection 2.2 – depicts this relationship graphically.

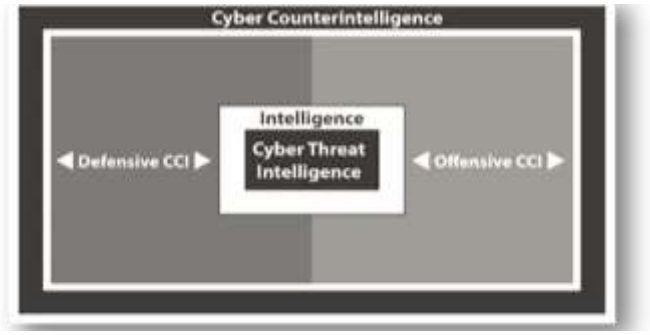


Figure 2: The relationship between Cyber Counterintelligence and Cyber Threat Intelligence (authors)

This section showed CCI as a multi-faceted CI sub-discipline that participates in, but extends beyond conventional cyber security. CCI was concluded to include CTI but to be much wider in respect of scope and nature of measures undertaken.

3. Towards a multi-layered CCI framework

Effective CCI is not only multi-facetted, but also stratified. To be optimal CCI needs to involve all organisational layers from the C-suite to line-functionaries. The levels conventionally ascribed to statutory intelligence –namely strategic, operational and tactical – provide a useful approach for explaining CCI. Although these levels are described in literature dealing with CTI, no postulation could be found in open-source literature on a multi-layered framework for CCI. Works of note in the CTI field include those by Mattern (et al 2014), Friedman & Bouchard (2015), Chismon & Ruks (2015) as well as a series of papers compiled by the Intelligence and National Security Alliance (INSA 2011, 2013, 2014a, 2014b, 2015). The cited works were foundational to the framework provided in Table 2 and were also applied for the subsequent narrative description of the CCI levels.

Table 2: A multi-layered CCI framework

	Strategic	Operational	Tactical/Technical
CI mission	• Advance and protect organisational interests through defence against, and the offensive engagement of, adversarial intelligence activities. This is achieved through the following functions: detect, deny, deter, deceive, degrade, and/or disrupt.		
CCI mission	• As above, when the adversary uses cyber as a conduit or a cyber asset is a target.		
Leadership	• C-level	• Senior & Middle Management	• Line and team leaders
Interface with CI	• Organisational, Intelligence and CI Strategies • All-source CI feed	• Multi-disciplinary programmes and operations	• Multi-disciplinary projects and continuous line-functional interaction
Referent objects	• Organisation's 'crown jewels' • Critical information and cyber-assets sought (e.g. adversary's 'crown jewels') • Conditions (competitive advantage)	• People, processes, systems, procedures (personal security, ICT architecture, supply-chain management) • Own intelligence programmes	• Systems, networks, and devices • Network Security Operations • C-I-A (confidentiality, integrity and availability)
Interrogatives	• Who, why?	• Who, Where, When, How?	• What, How?
Adversarial progression (Impact chain)	• Motivation, intent and decision, objective	• Objective • Avenue of Approach • Capability or perceived capability, develop access	• Develop network access, implement, assess, restrike • Payloads and payload delivery mechanisms
Level of adversarial role-player focussed	• Sponsors, opponents, Intelligence capacity	• Intelligence structures, groups, campaigns	• Individuals, TTPs, incidents, actions (on-the-network)

	Strategic	Operational	Tactical/Technical
Indicators of targeting and compromise	• Geo-political, sector/industry 'flags' • Analogous events • Adversarial strategy and business decisions	• Operational disruption • Organisational and/or revenue decline • Information leakage	• Breach in the CIA of cyber and / or information security milieu • Identification of malicious code, intrusion, threat exploitation
Analysis output	• High-level, strategic appraisals • Strategic warning and advisories	• Operational reports (CCI operations, threat, damage and vulnerability assessments, alerts, warnings) • Trend analyses	• Tactical and technical information reports • Alerts and warnings
Consumers of CCI products	• C-Level and operational management (selectively)	• Line-functional managers, CI analysts and CCI specialists.	• CCI analysts • CCI technical personnel
Means, methods and measures (Offensive, defensive and collection)	• Multi-discipline CI • Strategic direction of means, methods and measures in Table 1.	• As in Table 1 • Interlocked with operational and tactical CI.	
Cyber threat intelligence (Sourced)	• White papers, commissioned and non-commissioned research.	• Platforms.	• Data feeds.
Skillsets required (Line-functional)	• Sound knowledge of business and industry • Specialised knowledge and skills in Intelligence, multi-disciplinary CI and CCI • Strategic analysis and management	• Multi-disciplinary CI • CCI operational and/or technical specialisation • Operational management • Elements of both strategic and tactical	• ICT, information security • Systems, software development,programming, scripting, • Ethical hacking. • CI and CCI tactical /technical specialisation (also HUMINT) • Technical cyber defence and collection • Social sciences, languages • Engineering and Reverse Engineering

Within the confines of a conference paper, the framework above cannot be discussed in detail. Not even each of the vectors can be narratively explicated. The subsequent sub-sections thus do not rigidly mirror the table, but rather aim to provide a bird's eye view of the different levels on which CCI is executed.

3.1 Cyber counterintelligence on the strategic level

In his benchmark work, Prunckun 2012 rightly asserts "executive responsibility" as CI's "first and highest tenant". For CCI to be successful, the organisation's executive management (C-suite) need to understand and sanction CCI's mission to advance and protect organisational interests through defence against and the exploitation of adversarial, cyber-related intelligence activities (cf INSA 2014*b*, Chismon & Ruks 2015). Practically, the C-level executive assigned with leading the CI aspect will be responsible for also directing the CCI effort. The executive's responsibilities include obtaining the collective executive management's approval of CCI strategy, priorities and resourcing. In some instances the executive would selectively also seek endorsement – normally from the CEO – for high-risk and high-cost programmes. The actual CCI work on a strategic level is performed by a team consisting of seasoned CCI specialists, multi-disciplinary CI specialists, strategic analysts (business and CI) and various other experts relevant to the organisation's core business.

CCI informs the C-suite mainly through high-level products and presentations that include estimates, threat and risk assessments as well as advisories. These products are informed by appraisal all-source CI operational reports as well as an extensive all-source scanning of the macro-environment for CCI-relevant trends and drivers that could affect the organisation (INSA 2014*b*). External CTI products sourced would mainly be white papers as well as commissioned and non-commissioned research papers (Chismon & Ruks 2015). A thorough knowledge of organisational strategy and planning is imperative, as is a clear grasp of the organisation's information-related assets critical for it to exist and prosper – commonly referred to as the 'crown jewels' (INSA 2014*b*). It is these assets that CCI protects from adversarial intelligence activities and it is the organisational strategy that CCI should advance through the exploitation of adversaries in the cyber sphere.

Strategic CCI differs from that in the operational and tactical level in that it takes a wider view of the macro-environment and a longer term view on the actual or potential emergence of threats (Bodmer et

al 2012, Mattern et al 2014). Strategic CCI would for instance identify intelligence principals/sponsors who have plausible motive, intent and capacity to target the own organisation through cyber means. (See Table 2 – "Adversarial Progression") These principals or sponsors will not necessarily execute the actual intelligence activities but are they are the ultimate benefactors (such as a nation state). The actual implementers of hostile cyber as well as associated tactics are those that carry out the task of operational and tactical CCI. While the implementers will determine the operational and tactical avenue of approach, the strategic decisions (e.g. to pursue objectives via human and/or technical means) in this regard will be taken by the Intelligence principal. The pathway of adversarial progression guiding CCI therefore differs from that of CTI (compare Figure 1).

Strategic CCI is furthermore tasked with detecting high-level indicators that the organisation is being targeted or has been compromised. Similarly, strategic CCI should identify drivers and trends suggesting a rise in the risk of internal compromise (insider threat). Equally important is the detection that organisational strategy and decision-making are being unduly influenced by deceptive, adversarial cyber operations. Strategic CCI will advise on countermeasures to best exploit adversarial cyber activities. To be successful cyber counter-deception and exploitation have to be fully synchronised with such actions in other CI fields (such as agent and double agents operations). Therefore, it is imperative for CCI to ensure that countermeasures are aligned with CI and organisational strategy. The design and filling of honeypots on the operational and tactical levels, for example, will ultimately be informed by strategic CCI's direction on counter-deception (cf Bodmer et al 2012).

3.2 Cyber Counterintelligence on the operational level

As on the strategic level, CCI on the operational level strictly pursues the CCI's central mission of defensively and offensively advancing CI-relevant interests in the cyber sphere. Adherence to the mission at all three levels CCI ensures a coherent approach and an optimised CCI effort.

Operational CCI is driven by senior and middle management as well as specialists in the field of CCI operations and analysis. It functions as conduit and advisory to C-Level leadership in matters such as CCI strategic objectives, financials, financial projections and other resource requirements, projects, statistics and reporting.

Operational leadership is responsible, among other, for the following main functions (INSA 2014*a*, Mattern et al 2014): (i) operationalise the CCI strategy as set jointly by the executive management, operational management and CCI experts, (ii) develop and implement CCI structures and acquire resources, (iii) develop and implement operational plans and identify focus areas and (iv)drive daily operations and performance.

Operational CCI is responsible for safeguarding the people, processes, procedures and systems in which the organisation's critical cyber-related assets reside. Consequently, it includes a wide spectrum of organisational functions such as personal security, physical security, procurement, supply chain management, ICT-user management and much more. In addition to conducting CCI operations against adversaries (discussed below), it safeguards the organisation's own information and cyber intelligence operations. It provides operational cyber counterintelligence reports on operations, cyber threats and threat actors, damage and vulnerabilities (as identified through assessments), alerts, warnings and trends to the strategic CCI, line-functional managers, analysts and CCI specialist (Riley 2015). It also self-analyses the reports' output with a view to driving reports' outcomes to action (INSA 2013, 2014*a*).

Operational CCI interfaces with the larger CI function through multi-disciplinary programmes and operations, specifically focussing on the cyber part of CI. Its main concern is whom the adversaries are, their location, capabilities (such as the ability to utilise or develop malware), intentions (either pronounced or unpronounced) and modus operandi (Chismon & Ruks 2015). Together with this, it is concerned with the adversaries' intelligence structures and their intelligence campaigns (either planned or existing).

With regard to a traditional defensive approach, CCI similarly has a dual proactive-reactive focus to identify indicators of cyber targeting and compromise. Such indicators include a disruption in the organisational operations, tell-tale declines in organisational functionalities and/or information leakage. From a reactive perspective, CCI seeks to counter such instances by identifying its origin and addressing the compromise (through either defensive or offensive means). From a proactive approach, it identifies such possible capabilities and campaigns and addresses threats (by either defensive or offensive means)(Bardin 2011).

Operational CCI is persistently seeking exploitable opportunities presented by adversarial cyber campaigns, operations and actions. Through counter-operations these opportunities are pursued either pro-actively or re-actively – depending on the circumstances.

The skillsets required to capacitate operational CCI are multi-disciplinary and include elements such as general management, advanced operational management, CCI analysis, cyber security, cyber defence and offensive CCI techniques and other fields of technical expertise (Bodmer et al 2012).

3.3 Cyber counterintelligence on the tactical and technical levels

The aim of tactical and technical CCI is to achieve the organisations CCI mission though tactical and technical means. It is driven and executed by line-functional leadership as well as team leaders, role leaders, CCI technical and tactical experts, security analysts and other technical personnel. It has an advisory responsibility to both the operational and executive management that includes matters such as CCI threats and opportunities, defensive and offensive measures, systems and toolsets, CCI analyses and financials (Riley 2015; INSA 2013, 2015). This advisory responsibility is usually fulfilled through submitting tactical products to the operational and in some instances directly to the strategic CCI level. Prior to submission to the executive, tactical CCI inputs are normally contextualised at the operational and strategic levels.

Tactical CCI is responsible, among others, for the following main functions (cf INSA 2015): (i) concretise operational direction into action; (ii) identify, design and implement systems, toolsets and reporting mechanisms (both defensive and offensive), (iii) carry out tactical taskings through combined technical and HUMINT measures and (iv) identify, analyse and action CCI threats and opportunities.

Tactical CCI performs the daily management, configuration (including identification and/or compromise in the case of offensive measure implementation) of both defensive and offensive systems, networks, devices, network operations and security operations (INSA 2015). It is responsible for ensuring the C-I-A of the organisation's cyber and information security environment, as a defensive tactic and measure. In the case of an offensive or exploit tactic (that must be congruent with operational objectives and the organisational strategy) tactical CCI further strives to degrade the C-I-A of an adversary's cyber and information security. Tactical CCI interfaces with the larger CI function through multi-disciplinary projects and continuous line-functional interaction. Tactical and operational CCI has a shared focus on on-the-network threats and/or opportunities, threat actors' capabilities or possible capabilities as well as the deployment of and expansion of capabilities. Tactical CCI is concerned with engaging individual groups or individuals, their specific network actions, TTPs and specific technical issues such as malware signatures (Chismon & Ruks 2015).

Tactical and technical CCI processes feed into information reports and focus on specific issues such as breaches, the identification and/or creation of malicious code, intrusion, threat and exploitation. The process leads to the compilation of tactical and technical reports, alerts, warnings, defensive and offensive solution and action reports, campaign proposals, etc. These are provided to CCI analysts, tactical leadership, operational leadership and the executive in the manner described above (Friedman & Bouchard 2015).

The skillsets required for tactical and technical CCI are, as is the case with strategic and operational CCI, multi-disciplinary. They include elements of tactical and line-functional management, ICT security, development of systems and software, programming, scripting, developing offensive and defensive toolsets, CCI technical specialisation, HUMINT and intelligence collection, as well as language and social science expertise (used in for example penetration of hacking forums), ethical hacking, technical defensive and offensive measures as well as reverse engineering (Bodmer et al 2012).

4. Conclusion

This paper emphasised the centrality of CCI to engage morphing high-end cyber threats effectively. Although only well-resourced entities can afford a fully-fledged capacity in this field, a CCI mindset and approach could benefit smaller organisations. Within the context of CCI's infancy as an academic discipline, the paper sets out to contribute two further conceptual building blocks, namely a CCI–CTI differentiation and a multi-layered framework. Constructs such as these are important since they condition our approach to the practice. Since considerable further research is required, both constructs presented are qualified as tentative soundboards intended to stimulate future debate.

There is no consensus on definitions of CCI and CTI and this paper's differentiation is inevitably contestable. It nonetheless offers a start. The framework explicated activities on different organisational levels. As it stands, it provides more clarity on what CCI is and what it is supposed to do. With further research this framework can be developed to a scalable template for the practical execution of CCI on all organisational levels.

Acknowledgment
The research presented in this paper forms part of a project at the Centre for Cyber Security (Academy for Computer Science and Software Engineering, University of Johannesburg) aimed at formalising CCI as a multi-disciplinary field of academic inquiry in the South African context. Those interested are invited to contact the authors and/or view more detail at http://adam.uj.ac.za/csi/CyberCounterintelligence.html.

References

Bardin, J. (2011) "Ten commandments of cyber counterintelligence", *CSO* [online], http://www.csoonline.com/article/2136458/

Bodmer, S. A. et al (2012) *Reverse deception–Organized cyber threat counter- exploitation*, McGraw-Hill, New York.

Chismon, D. and Ruks, M. (2015), *Threat Intelligence: Collecting, Analysing, Evaluating*, MWR Infosecurity, UK Cert, United Kingdom.

CrowdStrike (2016) *Global Threat Report 2015* [online] www.crowdstrike.com/global-threat-report-2015/

Deloitte (2014) "Cyber threat Intelligence: Moving to an Intelligence-driven cybersecurity model." *Insight* , CIO edition, [online] http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-cyber-threat-intelligence-cybersecurity-29102014.pdf

Duvenage, P. C. and von Solms. S.H. (2015) "Cyber Counterintelligence: Back to the Future", *Journal of Information Warfare*, Vol. 13, Nr 1.

Duvenage, P.C, von Solms, S.H. and Corregedor, M (2015) "The Cyber Counterintelligence Process - a conceptual overview and theoretical proposition", Paper read at the 14th ECCWS, Hatfield, United Kingdom, July.

Duvenage, P. C. and von Solms. S.H. (2013) "The Case for Cyber Counterintelligence", Paper read at the 5TH Workshop on ICT Uses In Warfare and the Safeguarding of Peace, Pretoria, South Africa, November.

EMC² (2014) *Intelligence Driven Threat Detection and Response (White paper)*, [online], https://www.emc.com/collateral/white-paper/h1304-intelligence-driven-threat-detection-response-wp.pdf

Friedman, J. and Bouchard,M. (2015) Definitive Guide to Cyber Threat Intelligence, [online], https://cryptome.org/2015/09/cti-guide.pdf

Godson, R. (2001) *Dirty tricks or trump cards - U.S. covert action and counterintelligence*. Transaction Publishers, New Brunswick.

Google (2016), Search "threat+intelligence", (2016-02-16)

Info-security Magazine (2015) "Global threat intelligence services spending is projected to rise", [online], **http://www.infosecurity-magazine.com/news/cybersecurity-spending-to-hit/**

INSA -Intelligence and National Security Alliance (2015*a*), *Tactical Cyber Intelligence*, online, http://www.insaonline.org/i/d/a/b/TacticalCyber.aspx

INSA(2014 *a)*, *Operational Cyber Intelligence,* [online] www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx

INSA (2014 *b) Strategic Cyber Intelligence*, [online] www.insaonline.org/i/d/a/b/StrategicCyberWP.aspx

INSA (2013) *Operational Levels of Cyber Intelligence*, [online], http://issuu.com/insalliance/docs/_insa_wp_cyberintelligence_pages_hir/16?e= 6126110/4859250

INSA (2011) *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*, [online] www.oss-institute.org/storage/.../insa_cyber_intelligence_2011.pdf

iSightpartners (2014) *What is Cyber Threat Intelligence and why do I need it?* [online], http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief 1.pdf

Kaspersky (2015) *Global IT Security Risks Survey 2015: The current state of play* [online] http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf

KPMG (2013) *Cyber threat intelligence and the lessons from law enforcement*, [online] http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-threat-intelligence-final3.pdf

Lee, R. M. (2014a) "Cyber Threat Intelligence". *Tripwire* ,blog series, part 5. Retrieved on 04 January 2015 from http://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/

Lee, R. M. (2014b), "Cyber Counterintelligence: From Theory to Practice". *Tripwire*, blog series, part 4. Retrieved on 04 January 2015 from http://www.tripwire.com/state-of-security/.../cyber-counterintelligence-from-theory-to-practice/

Mattern, T. et al (2014) "Operational Levels of Cyber Intelligence", *International Journal of Intelligence and Counterintelligence*, vol. 27, no. 4.

McAfee Labs (2015) 2016 Threats Predictions http://www.mcafee.com/us/resources/reports/....predictions-2016.pdf
Moyo, A. (2015) "Syndicates wreak havoc in cyber space", *ITWeb*, [online] http://www.itweb.co.za/index.php?option =com_content&view=article&id=143480:Syndicates-wreak-havoc-in-cyber-space&catid=234
PwC (2016) *Global Economic Crime Survey 2016: The UK*, [online], http://www.pwc.co.uk/gecs
Prunckun, H (2012) *Counterintelligence: Theory and Practice*, Rowman & Little Publishers, Plymouth.
Riley, S. (2015) Insights *to Modern Threat Intelligence*, online, https://www.linkedin.com/pulse/insights-modern-cyber-threat-intelligence-shawn-riley?articleId=7011683228767036224
Schoeman, A. (2015)"Demystifying Threat Intelligence", *Infosecurity Magazine*, [online], http://www.infosecurity-magazine.com/opinions/demystifying-threat-intelligence/
SpearTip (2015) Cyber *Hunt Team Operations and Counterintelligence*, [online] http://www.iopw.com/Article/9461/Business--Professional-Services/Cyber-Hunt-Team-Operations-and-Counterintelligence?gPage=60
Statista (2016) *Threat Intelligence Services Worldwide*, [online], www.statista.com/statistics/417588/threat-intelligence-spending/...../
The Economist (2015) "*Counter-intelligence techniques may help firms protect themselves against cyber-attacks", [online],* http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protectthemselves
VeriSign (2012) *Establishing a Formal Cyber Intelligence Capability,* (White Paper), [online], https://www.verisigninc.com/assets/whitepaper-idefense-cyber-intel.pdf.

ANNEXURE F

UCD Forensics and Security Research Group

UCD DUBLIN

Proceedings of the 16th European Conference on Cyber Warfare and Security

University College Dublin
Ireland
29-30 June 2017

Edited by
Dr. Mark Scanlon and Dr. Nhien-An Le-Khac
University College Dublin

acpi

A conference managed by ACPI, UK

Review Process
Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy
ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here: http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academic-conferences-and-publishing-international-limited/

Conference Proceedings
The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

The Electronic version of the Conference Proceedings is available to download from DROPBOX http://tinyurl.com/ECDAS2017. Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.
The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISSN: 978-1-911218-44-9
E-Book ISSN: 2048-8610
Book version ISBN: 978-1-911218-43-2
Book Version ISSN: 2048-8602

Published by Academic Conferences and Publishing International Limited
Reading
UK
44-118-972-4148
www.academic-publishing.org

A Conceptual Framework for Cyber Counterintelligence – theory that really matters

Petrus Duvenage[1], Thenjiwe Sithole[2], Sebastian von Solms[3]
[1] Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa
[2] Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa
[3] Centre for Cyber Security, University of Johannesburg, South Africa

duvenage@live.co.za
thenjiwes@icloud.com
basievs@uj.ac.za

For those connecting the dots, major cyber breaches continue to affirm the necessity of having cyber counterintelligence (CCI) at the core of a proactive cybersecurity approach. While practitioners and executives engaging high-end adversaries in the 'real world' are progressively warming up to the opportunities CCI presents, the mentioning of 'theory' is likely to evoke a cool response. Theory is typically regarded as abstract thinking that has little bearing on, or use in, 'real world' cybersecurity trenches. Theory may even be deemed to be the opposite of practice. This is of course not the case – theory is highly relevant to practice and practice ought to inform theory. In the words of Lewin (as cited by Greenwald 2012): "There is nothing so practical as a good theory."

Especially for a field as complex as CCI, effective practice presupposes a sound theoretical foundation. The price for poor CCI theory will ultimately be paid through more costly failures and damaging breaches. Theoretical constructs are thus clearly not 'nice to have' academic 'toys'. These constructs, which include frameworks and models, condition our thinking and our approach to practice. In addition to its application to practice, theory should of course also be at the heart of academic disciplines and fields.

Herein lies the challenge – as an emerging multi-disciplinary academic field, CCI is in its infancy. Given CCI's incipient status, one of the priority agenda items ought to be a conceptual framework that (albeit tentatively) delineates and provides a coherent view of the research object – i.e. CCI. This conceptual framework can furthermore systemise existing knowledge and provide a scaffold for further research. Equally important, it can be an instrument to explain to diverse audiences what CCI is and how it works. Clearly then, a conceptual framework for CCI is theory that really matters.

This paper's primary aim is to advance the outlines of such a conceptual Framework for CCI (FCCI). Our FCCI consists of eight notional blocks we deem essential to an academic credible and practically useful FCCI. In designing the FCCI, we synthesised and added to previous contributions on CCI to inter alia recent European Conferences on Cyberwarfare and Security (ECCWS).

For obvious reasons, the FCCI and its building blocks cannot be explained in any detail within the confines of a single conference paper. Consequently, suffice it to provide the essential contours of, and rationale behind, our FCCI's design. We qualify our FCCI as a tentative postulation, hopefully constructive to the theoretical discourse and academic practice.

Keywords: cyber counterintelligence, theory, offensive cybersecurity, active defence, conceptual framework.

1. Introduction

For those connecting the dots, several recent cyber breaches have affirmed what we have known for more than two decades – state and non-state actors' use of the cyber sphere for Intelligence operations is set to continue to increase sharply (cf. Molander et al 1996, Stroz Friedberg 2017). While the motives for such Intelligence operations vary from the influencing of world politics and cyber espionage to pure criminal gains, the distinction between modus operandi and tradecraft is blurring (Crowdstrike 2016). Some of the better known 2016 incidents attesting to this trend include the hacking of Bangladesh Bank, the US Democratic Party National Convention and Yahoo.

These, and numerous other breaches, underline anew the necessity of having cyber counterintelligence (CCI) at the core of a proactive cybersecurity approach. CCI is now more relevant than ever before and can be expected to gain further traction in the boardrooms of companies with sizable assets (Jaquire 2017, SpearTip 2015, The Economist 2015). CCI is, however, not a quick-fix solution. It is not a neat plug-in or add-on that starts and ends with on-the-network actions. Like cybersecurity in general, CCI is anchored in our organisational DNA. Effective CCI also presupposes a profound understanding of long-established Intelligence and Counterintelligence concepts. Yet, and although "practised by state security structures for over twenty years, CCI remains poorly understood in the public and commercial domains." (Duvenage, von Solms & Corregedor 2015). Academic theory and research can of course play a pivotal role in this regard. However, we have a dilemma – we need CCI theory to inform sound practice but such theory is lacking. This paper aims to contribute a conceptual Framework for Cyber Counterintelligence (FCCI) as a construct, hopefully useful to this field's academic development and practice.

To be academically credible, we need to explain and contextualise our approach to the FCCI's design. This is addressed in Section 2 and 3. Section 2 defines a 'conceptual framework' and describes how this fits in with 'theory' (Section 2). We then proceed with discussing the requirements to which the FCCI's design should comply (Section 3). Guided by these requirements, we then present the outlines of the FCCI and its eight building blocks (Section 4). The FCCI we present synthesises, develops and adds to previous contributions on CCI (Duvenage & von Solms 2013; Duvenage & von Solms 2015; Duvenage von Solms & Corregedor 2015, Duvenage, Jaquire & von Solms 2016). Since we, within the confines of a conference paper, only provide a bird's eye view of the FCCI's contours and then conclude with observations on further research (Section 5).

2. What is a 'Conceptual Framework' and how does it fit in with 'theory'?

Since it will impact on the design of our FCCI, we have to be clear on what a 'conceptual framework' is and how this fits in with 'theory'. To this end, this section firstly reflects on the notion 'theory' and then proceeds to define a 'conceptual framework'. We concluded by applying this definition and positioning to the FCCI.

In a general sense, **'theory'** can be described as the interrelated collective of definitions, concepts, constructs (i.a. models and frameworks) as well as propositions to explain and understand a phenomenon/phenomena and/or aspects thereof. It is important to note that the 'theory' of an academic subject is not always a homogeneous body of thinking, but more often competing bodies of thinking. These bodies of thinking vary in their focuses from the abstract and broad to the more concrete and specific. Postulations on the meta-paradigm and paradigmatic levels are abstract and broad in scope, while meso-theories are more concrete and specific. These layers of theories' different purposes are aptly summarised by Gill (2006) in his distinction between "theories *of* intelligence" and "theories *for* intelligence". Theories of intelligence asserts Gill (2006), are developed to "help academics research intelligence, come to understand it, and better explain it". Theories for intelligence "relate immediately to the needs of practitioners" ... In one sense there is no conflict between these two. A good theory of intelligence should, by definition, be useful for intelligence".

Within the above context, we can broadly define a **'conceptual framework'** as a theoretical construct that narratively and/or graphically conveys the "essential or underlying structure, a provisional design, an outline; a connectional scheme or system" of a particular study object (Oxford Dictionary 2016). While a conceptual framework is per definition skeletal and tentative, it can nonetheless "provide a comprehensive understanding of a phenomenon... Conceptual frameworks are [thus] not merely collections of concepts but, rather, constructs in which each concept plays and integral role" (Jabareen 2009). A conceptual framework can serve as (i) a theory of a study object, (ii) theory for a discipline and (iii) a combination of these two.

Moving from this general definition, we define the **FCCI** simply as a theoretical schema that explains CCI by means of a collection of concepts (i.e. building blocks). As will be shown in Section 4, the FCCI is for the most part a theory *for* CCI, but also includes elements of abstract, higher-order theories.

3. A 'Conceptual Framework for Cyber Counterintelligence' – what it should do and why it matters?

The foregoing description of a conceptual framework provides us with a foundation for deriving the requirements to which our FCCI should comply. Essentially, the requirements are a response to the question: What should the FCCI look like and what should it be able to do (functions)? The requirements will guide the design of our FCCI's design in Section 4. Ultimately the application of these requirements determines the FCCI's effectiveness, uses and benefits. It is these benefits that demonstrate why the FCCI is a theoretical construct that ought to matter for academics and practitioners.

The FCCI's requirements, functions and benefits are closely related and overlapping. In the interest of simplicity we addressed all these by means of the following consolidated list in which we assert that the FCCI should:

- Be academically credible and practically useful.
- Graphically and narratively, describe what CCI is, of what it comprises (building blocks) and how it works.
- Be simultaneously "congruent *with* reality and an idealised, simplified representation *of* reality." (Duvenage, von Solms, Corregedor, 2015). Since it is an idealisation, the FFCI has to be an aiming point of what CCI should encapsulate if executed flawlessly.
- Serve as a conceptual template for CCI practice and its synergetic execution with the broader organisational endeavour.
- Be a nexus for linking CCI with other fields of practice and multi-disciplinary academic enquiry.
- Position itself as part of the theoretical discourse.
- Be scalable in that it should be able to explain CCI on the strategic, operational, tactical and technical layers.
- Serve as a scaffold to structure knowledge and research.
- Be derived through a qualitative (grounded theory) process that draws on the researcher's experiential knowledge, existing theory and research.
- Be qualified as a tentative artefact that is subject to validation and constant modification.

In this part of the paper we listed some aspects that can guide the design of our FCCI. This design is the focus of the next section.

4. An outline of the conceptual Framework for Cyber Counterintelligence (FCCI)

This section designs and presents an outline of the FCCI. We present the FCCI by means of a progressive block-by-block construction of the framework. At each of the respective building blocks, we:

- Graphically, depict the addition of the building block to the FCCI.
- Explain why the particular building block is essential to our FCCI.
- Offer a cursory outline (contours) of the building block in question. This outline comprises of a concise description/definition of concepts and a brief mentioning of facets that can direct further research and theorisation.

The paragraph above described our approach to presenting the FCCI in this paper. We now proceed with discussing the first building block namely a 'Theoretical Anchor'.

4.1 Building Block 1: Theoretical Anchor

Graphically the FCCI's theoretical anchor can be depicted as follows:

Figure 1: Building Block 1 – Theoretical Anchor

4.1.1 Why is this building block needed?

To be academically credible the FCCI has to duly consider, and position itself as part of the existing theoretical discourse. Such anchoring provides a nexus for linking CCI with other academic fields. The anchoring of our FCCI in theory is also important from a practical point of view. As was noted earlier, theory conditions our thinking and thus our approach to practice. Consequently, the theoretical anchor will determine both the way in which we design the rest of our FFCI and ultimately CCI practice.

4.1.2 Building block contours

Section 2 and 3 explained the FCCI predominantly as a theory on a lower level of abstraction. Accordingly, the FCCI's first building block comprises the linking of the FCCI with levels of higher abstraction, namely on the meta-paradigmatic, paradigmatic, theory and meso-theory levels. The building block has to clearly indicate the core theoretical contentions on which the FCCI is based.

Although CCI is a multi-disciplinary field, it has its primary taproot within Intelligence Study and Political Science (notably International Relations) theory. Intelligence and Political Science theory is of course not a homogenous body of thinking and the discourse is one of competing narratives that include inter alia Realism, Liberalism, Constructivism, Radicalism, Poststructuralists and Critical Realism. In our view, Realism best explains Intelligence, CI and CCI (cf. Duvenage & Hough 2011). Through a Realist lens, the contours of the FCCI's first building blocks are as follow:

- On the **meta-paradigmatic** level, we subscribe to a **Positivist** position. An objective world (reality) is deemed to exist separately from the researcher/practitioner. Extended to the FCCI, we assert that this framework can objectively identify, describe and guide the pro-active mitigation of 'real' threats and risks to the Organisation.
- On the paradigmatic layer, we take a **Realist** stance as was mentioned prior. Accordingly, the state (or more generically the 'Organisation') is seen as a rational, self-interested entity driven by the pursuit of its security and expanding its vital interests vis-à-vis other actors. The Organisation's relative power is a key factor in this quest. These vital interests are pursued against other actors in the political, social, technological, economic, military, ecological (environmental) and information sectors. Intelligence and cyber form part of the information sector.
- Extending Realism to the **Grand Theory** level, we view **Intelligence** as simultaneously a class of vital interests and category of power. Within this context 'cyber' is exponentially increasing its centrality as a tool and asset.
- On the **meso-level**, **Counterintelligence** and therefore CCI, is the Intelligence element tasked with protecting and advancing the Organisation's interests in the face of other role-players' hostile Intelligence actions.

Properly designed the first building block presented above serves as a theoretical roadmap for the design of further FCCI building blocks. Since building blocks repeat and expand different theoretical positions, building block 1 acts as the central notional node that binds all further FCCI theory. It is the anchor to which we constantly refer back.

4.2 Building Block 2: Organisation

With the CCI theoretically anchored, the FCCI's pivot that is the Organisation can be constructed. Graphically, we can depict this building block as follows:

Figure 2: Building Block 2 – The Organisation

4.2.1 Why is the building block needed?

The Organisation is advanced as the FCCI's pivot for reasons of theory and practicality. In line with our Realist theoretical position, the Organisation and the pursuance of its interests predominate. Seen through this lens, CCI is ultimately about maximizing the Organisation's power through protecting and advancing interests. Therefore CCI exists because of, and for the organisation, it serves. Also practically,

effective CCI crucially depends on a profound knowledge of the Organisation. Against sophisticated adversaries, for example, the Organisation's staging of honeynets and the content filling of honeypots, honeyfiles and honeytokens have to be attuned to the Organisation's itself, its adversaries and its environment (Bodmer et al 2012, Duvenage & von Solms 2013).

4.2.2 Some building block contours

The 'Organisation' is a generic concept that can refer to various types of entities, ranging from nation states and multi-national corporates to smaller businesses and non-governmental organisations. Regardless of the type of entity we are dealing with, aspects to be addressed in explicating the Organisation as an FCCI building block are the following:

- The Organisation's **vision, goals** and the **vital interests** it wants to protect and procure in order to be more secure and prosperous. Although these vital interests exist in various domains, it is central to the later configuration of the CCI effort, to identify and concretely describe **vital informational interests**.
- The Organisation's **strategy** for pursuing its vision and objectives.
- Organisational **strengths** (inclusive of the vital interests and instruments of power it possesses) and **weaknesses** (vulnerabilities). Also in this case, particular attention should be given to the information sphere.
- The **environmen**t in which the Organisation functions. Of particular importance are the implications of current as well as anticipated trends on the Organisation reaching its objectives and expanding prosperity.
- Actual and potential **competitors/adversaries** and, also in this instance, the implications thereof on the Organisation attaining its objectives.

This subsection discussed the addition of the 'Organisation' as an FCCI building block. We emphasised the importance of being clear about the Organisation 's **Interests**, **Gaols** and **Strateg**y (**IGS** – se Figure 4, Subsection 4.3.2). Within the context of the latter, CCI is but part of a much broader organisational endeavour, namely Intelligence. In the next subsection we therefore propose Intelligence as the FCCI's subsequent building block.

4.3 Building Block 3: Intelligence ('toolkit')

Graphically, the addition of Intelligence as an FCCI building block can be depicted as follows:

Figure 3: Building Block 3 – Intelligence

4.3.1 Why the building block is needed?

While an indispensable instrument, CCI cannot secure and pursue an Organisation's interests all by, and for, itself. This has to be done as part of an Organisation's Intelligence endeavour. CCI, by way of analogy, is but one 'tool type' within an Organisation's Intelligence 'toolkit'. Academia and practitioners serious about CCI have to have a sound grasp of Intelligence (toolkit) as well as Intelligence's three toolsets (Positive Intelligence, Covert Action and Counterintelligence). Since these are also performed within CCI, clarity is furthermore needed on Intelligence functions (such as management, analysis and collection).

4.3.2 Building Block contours

In order to contour 'Intelligence' as an FCCI building block, it needs to be defined. With the qualification that there is no commonly accepted description, we define '**Intelligence**' as:

> the process by which specific types of information important to an Organisation's vital interests are requested, collected, analysed, and provided to the decision makers, the products of that

process; the safeguarding and advancement of informational interests by counterintelligence activities; and the carrying out of other sanctioned informational operations (Lowenthal 2012, Godson 2001).

Underpinning the definition is the notion that Intelligence (toolkit) consists of the three interrelated elements (toolsets). As part of our contouring, we now very briefly describe the **three Intelligence elements** (Duvenage, von Solms, Corregedor 2015):

- **Positive Intelligence** aims to provide information "to facilitate one's own side achieving its ends." (Bodmer et al 2012). This information varies from analysed open-sources to opponents' secrets obtained through espionage.
- **Covert action** targets an adversary through the influencing of events, conditions, individuals, groups or institutions to the benefit of the client in a manner not attributable to the sponsor or at least offering plausible deniability (Duvenage, von Solms, and Corregedor 2015). In the information sphere, covert action can take the form of propaganda, deception and denial, disinformation and perception management.
- **Counterintelligence** is an abbreviated form for the countering of hostile intelligence activities and it is discussed in more detail in subsection 4.4

Traversing and performed in all toolsets, are specialised **Intelligence functions** such as management, analysis and collection. These Intelligence functions, which are also performed within CCI, bind the three Intelligence elements.

Diagrammatically this relationship can be depicted as follow:

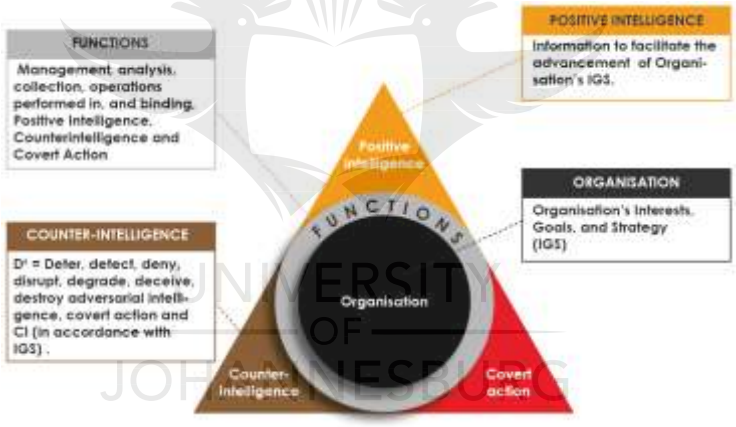


Figure 4: Intelligence and its three elements – Positive Intelligence, counterintelligence and covert action

Since the foregoing explanation is but a cursory contour, it risks being an oversimplification. A thorough explication of Intelligence as an FCCI building block will have to describe concretely the synergy between, on the one hand CCI, and, on the other hand, Intelligence elements and functions. It will explain how CCI depends on and benefits from all three Intelligence elements. Of these elements, and for reasons discussed below (Section 4.4), counterintelligence and its relation with CCI are of particular importance. So important in fact, that Counterintelligence is advanced in the next section as a distinctive CCI building block.

4.4 Building Block 4: Counterintelligence ('Toolset')

Graphically, the addition of Counterintelligence (CI) as the FCCI's fourth building block can be depicted as follows:

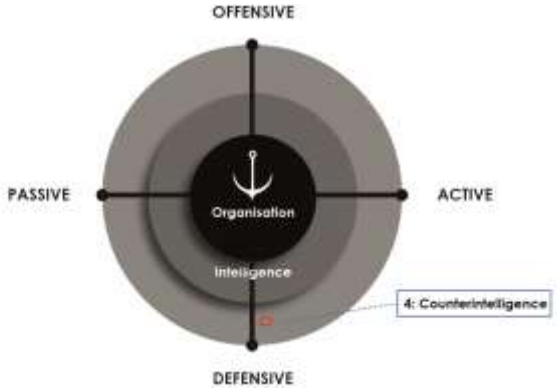


Figure 5: Building Block 4 – Counterintelligence

4.4.1 Why the building block is needed?

In the preceding section we positioned CI (and thus CCI) as part of an Organisation's Intelligence endeavour. In this section we advance CI as the subsequent building block of our FCCI because we cannot conceptually structure and understand CCI, if we do not understand CI of which CCI is part. CCI is by way of analogy one of the 'tool types' within the CI 'toolset'. Practically and conceptually, CCI is linked with the whole of the multidisciplinary CI effort. CCI is, in other words, not a neat compartment within CI. It involves, and requires clarity of, all other CI fields.

4.4.2 Some building block contours

To delineate CI as an FCCI building block, we also in this instance offer a definition. Expanding on earlier contributions (Duvenage & von Solms, 2013; Duvenage, Jaquire & von Solms, 2016), we define CI for purposes of this paper as the collective of measures an Organisation undertakes to identify, deter, exploit, degrade, neutralise and protect against adversarial intelligence activities and internal risks deemed as detrimental or potentially detrimental to the organisation's vital informational interests and the pursuance thereof. Such hostile intelligence actions "include espionage as well as other actions that could degrade the integrity and/or availability of valued information, information systems and processes" (Duvenage & von Solms 2013). Differently phrased, the adversarial intelligence that CI engages comprises of adversarial positive intelligence (inter alia espionage), covert action and adversarial CI. To perform this role, CI relies on a wide range of measures. CCI is involved in, and is in some way or another, reliant on most CI measures (see third bullet in paragraph below – Five clusters of CI measures).

In order to explain CCI, this building block has to describe CCI's link and relation with the whole of the CI endeavour. To this end, aspects that have to be addressed and their application to cyber explained, include but are not limited to the following:

- CI **principles** and doctrine.
- CI's offensive and defensive **missions** as well as CI's passive and active **modes** (Prunckun 2012, Duvenage & von Solms 2015, Duvenage, Jacquire & von Solms, 2016).
- The clusters of **CI measures** namely (i) Physical Security, (ii) Information and Technological Systems Security, (iii) Personnel Security, (iv) Counterintelligence Monitoring, Investigation, and Collection; and (vi) Counterintelligence Exploitation, Deception and Neutralisation (Prunkun 2012, Duvenage 2013, Prunckun 2012).
- The difference and interplay between **strategic, operational** and **tactical CI** (Duvenage, Jacquire & von Solms, 2016).

In this section CI was advanced as an FCCI building block. In the next section we submit the FCCI fifth component, namely CCI.

4.5 Building Block 5: Cyber Counterintelligence ('Tool type')

The addition of CCI as the FCCI fifth building block can be graphically illustrated as follows:

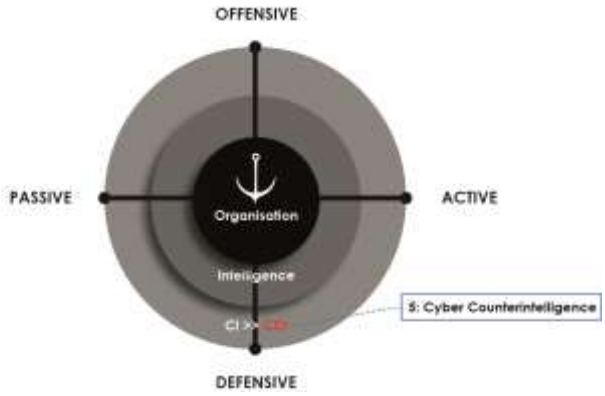


Figure 6: Building Block 5 – Cyber Counterintelligence

4.5.1 Why the building block is needed?

In order to illustrate the interlock between CI and CCI, the diagram above deliberately depicts the two fields in the same ring and on the same level. This is done to graphically reflect this paper's recurring theme namely that CCI is but a tool type within the broader CI toolset. Hence, CCI is defined as "that subset of multi-disciplinary CI aimed at detecting, deterring, preventing, degrading, exploiting and the neutralisation of adversarial attempts to collect, alter or in any other way breach the C-I-A [confidentiality, integrity and availability] of valued information assets through cyber means and/or where cyber assets are targeted" (Duvenage, von Solms, Corregedor 2015). As is clear from this definition and the term *Cyber* Counterintelligence, this FCCI building block **explicates CCI a as a technical toolset**. This toolset comprises of an extensive range of tools (technologies, measures and techniques). Most of these tools are not unique to CCI. What is unique, is the application thereof in combination with other CI tools and in a manner best achieving CI's missions.

4.5.2 Some building block contours

A more detailed explication of CCI as an FCCI building would therefore entail the describing of the application to the CI context of the said technologies, measures and technologies. The following serve as some examples (Bodmer *et al* 2012, Heckman *et al* 2015, Jaquire 2017):

▪ Host–based tools (Antivirus, Digital forensics, Security management tools) ▪ Network-based Tools (Firewall, IDS/IPS) ▪ Incident Management and coordination (Detection, Analyses, Response, Recovery) ▪ Profiling, Attribution and Decisions models. ▪ Data mining, modelling and reporting tools ▪ Sock puppets as tools of collection, deception, influencing and neutralisation. ▪ Scripting, penetration, hacking and exploitation	▪ Active engagement procedures (Internal and External to network). ▪ Denial and Deception Technologies (tarpits, black holes, honeynets, honeywalls, content staging and filling). ▪ Malware analysis, engineering, reverse engineering and development. ▪ Insider Cyber Threat Mitigation tools and measures. ▪ Cyber Supply Chain (Allied to CCI - Threats and Opportunities)

This subsection advanced and contoured CCI as an FCCI building block. The next subsection adds the CCI matrix as a further building block.

4.6 Building Block 6: CCI Matrix

Graphically the adding of the CCI matrix to the FCCI can be illustrated as follows:

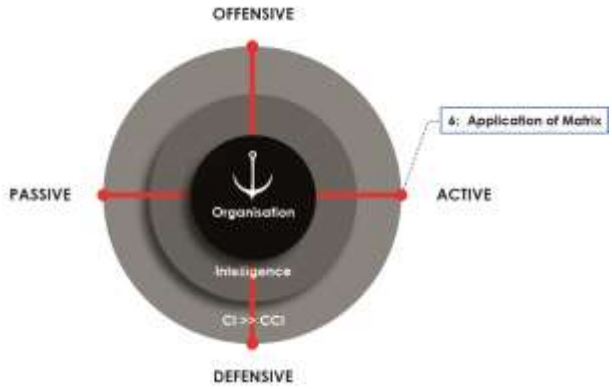


Figure 7: Building Block 6 – Application of the CCI Matrix

4.6.1 Why the building block is needed?

Subsection 5.5 noted that CCI tools should be used in a manner best achieving CI offensive and defensive missions. CCI tools can seldom be pigeonholed as having only a defensive or an offensive purpose. In various instances they can be useful to more than one. Furthermore, a significant part of tools can be deployed in an active or passive mode. To add to the complexity, effective CCI requires the integrated execution of offensive/active and defensive/passive modes. They can, after all, be described as different sides of a cube. The configuration of the CCI's passive-active and defensive-offensive endeavour is complex and unique to each Organisation. In order to explain and guide this configuration, we require a conceptual construct as part of the FCCI.

4.6.2 Some building block contours

To meet this requirement, the FCCI advances, a **four-quadrant matrix** as such a conceptual construct. This matrix explains the defensive-offensive and active-passive CCI postures. Similar to several other constructs, this matrix is derived from multi-disciplinary CI. A more detailed description of the matrix as an FCCI building block would firstly involve the narrative description of each of the four quadrants. Secondly, the matrix will have to be populated with the CCI tools available, and in accordance with the CI needs of the Organisation. Concretely the matrix's population entails the plotting on the matrix of CCI tools. Ideally, the plotting of the matrix can be informed by **taxonomy of CCI tools** (for a more detailed explanation of the matrix and taxonomy see Duvenage, Jaquire & von Solms 2015, Duvenage & von Solms 2015).

In this subsection, the CCI matrix was explicated as the FCCI's sixth building block and we now proceed with introducing 'Delineation and Cooperation' as the next component.

4.7 Building Block 7: Delineation and Cooperation

We can illustrate the addition of 'Delineation and Cooperation' as the FFCI's next building block as follows:

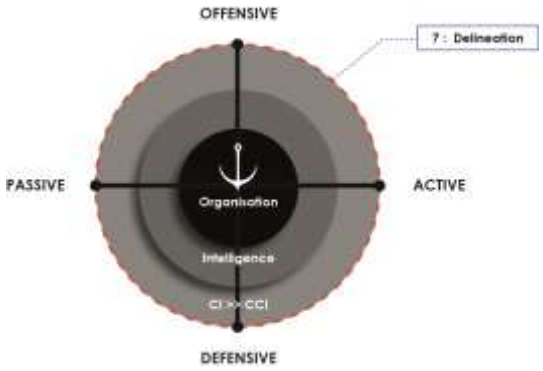


Figure 8: Building Block 7 – Delineation and Cooperation

4.7.1 Why this building block is needed?

By its very nature, the cyber-sphere is one of an interconnected reality. Even with all the previous building blocks in place, an Organisation would seldom be able, or legally allowed, to execute the whole of the CCI endeavour on its own. Business entities would, for example, be legally prohibited and not have the resources to undertake some active-offensive cyber campaigns undertaken by nation-states. In a similar vein, nation-states have to cooperate with non-state actors to achieve national goals. Consequently and although ultimately driven by each actor's self-centred interests, effective CCI requires cooperation with other actors and a delineating respective roles.
Delineation is also important in the academic context. Treating CCI as a too wide and encompassing field will result in the loss of focus. Simultaneously, CCI must be clear on its relation with various other academic subjects and on the areas of multi-disciplinary research.

4.7.2 Some building block contours
The 'Delineation and Cooperation' building block typically consists of a narrative description of areas of cooperation. In the academic arena, comparative studies and multi-disciplinary research are useful for refining CCI's focus and exploring areas of cooperation.
In this part, we proposed 'Delineation and Cooperation' as the FCCI's seventh building block. In the subsection to follow, we discuss the FCCI's last building block, namely the CCI process.

4.8 Building Block 8: CCI Process
The addition of the CCI Process as the FCCI's eighth and last building block can be depicted as follows:

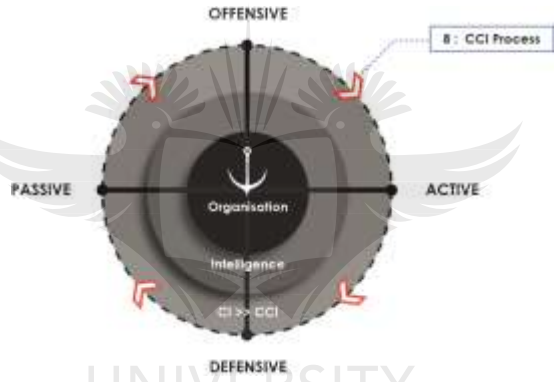


Figure 9: Building Block 8 – The Conceptual Framework for Cyber Counterintelligence

4.8.1 Why this building block is needed?
Properly contextualised, the foregoing building blocks provide all the 'parts' necessary to academically explain and practically execute CCI. At this juncture, these parts – and thus the FCCI – are still 'static'. They lack the dynamism that synergistically combines and drives these different parts as an integrated process. Consequently, the FCCI proposes a CCI process model as its last component.

4.8.2 Some building block contours
A process model typically consists of a graphically depicted and narratively explained step-by-step action. Seeing that its part of Intelligence and CI, the design of the CCI process has to consider existing propositions on the Intelligence, CI and CCI processes. In a previous contribution, the authors evaluated some salient existing propositions and found that these do not sufficiently explain CCI (Duvenage, von Solms & Corregedor 2015). These propositions, neither "reflect the defensive and offensive counterintelligence thrusts" nor are they "granulated enough to serve … as an aiming point for practical execution or a sounding board for further academic exploration" of a CCI process model (Duvenage, von Solms & Corregedor 2015). The said authors proceeded with presenting the contours of a process model that consists of a flow diagram and a narrative description of the CCI process. This model, albeit on a high level, provides the contours of a workable CCI process model.
In this section we presented our FCCI by means of progressive block-by-block construction. In the next section, we conclude with observations on ongoing and further research.

5. Conclusion

This paper set out to present the approach to, and outlines of, a conceptual Framework for Cyber Counterintelligence (FCCI).In the 'real world' of cybersecurity practice, CCI is an intricate field. CCI is distinctive from, yet intertwined with, various other specialisation fields. Its successful execution, therefore, depends on diverse skillsets. Within this diversity and intricacy, we risk losing clarity and focus. The FCCI we advanced is hopefully a simplified notional construct with some explanatory power.

The FCCI has been qualified as tentative proposition and subject to refinement. This refinement requires constructive criticism and further research. Our current research is focussed on a more detailed explanation of the FCCI and subjecting this research to cross-disciplinary peer review. Feedback received so far is positive and the FCCI is currently being used as the basis for a CCI maturity model. We also foresee in the near future to use a considerably expanded FCCI as the basis for a multi-tiered CCI training programme.

References

Bodmer, S. A. et al (2012) *Reverse deception–Organized cyber threat counter- exploitation*, McGraw-Hill, New York.

CrowdStrike (2016) Global Threat Report 2015 [online] www.crowdstrike.com/global-threat-report-2015/

Duvenage, P.C. (2013) "Counterintelligence," in Prunckun, H (ed.), *Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries*, Charles C. Thomas, Springfield IL.

Duvenage, P.C. (2017) *A Conceptual Framework for Cyber Counterintelligence*, in-progress dissertation towards an M.Com (Informatics) at the Academy of Computer Science and Software Engineering, University of Johannesburg.

Duvenage, P.C. & Hough, M 2011, 'The conceptual structuring of the intelligence and the counterintelligence processes: Enduring holy grails or crumbling axioms–quo vadis?' *Strategic Review for Southern Africa, University of Pretoria, Pretoria*, Vol. 33, Nr 2.

Duvenage, P.C., Von Solms, S. H. and Jaquire, V.J. (2016) "Conceptualising Cyber Counterintelligence – Two Tentative Building Blocks", *15th European Conference on Cyber Warfare and Security*, published conference proceedings, Munich, Germany.

Duvenage, P. C. and Von Solms. S.H. (2015) "Cyber Counterintelligence: Back to the Future", *Journal of Information Warfare*, Vol. 13, Nr 1.

Duvenage, P. C., Von Solms, S.H. and Corregedor, M. (2015) "The Cyber Counterintelligence Process - a conceptual overview and theoretical proposition", *14th European Conference on Cyber Warfare and Security*, Hatfield, United Kingdom, July.

Duvenage, P. C. and Von Solms. S.H. (2015) "Cyber Counterintelligence: Back to the Future", *Journal of Information Warfare*, Vol. 13, Issue 4.

Duvenage, P. C. and von Solms. S.H. (2014) "Putting Counterintelligence in Cyber Counterintelligence", *13th European Conference on Cyber Warfare and Security*, published conference proceedings, Piraeus, Greece.

Duvenage, P. C. and Von Solms S.H. (2013) "The Case for Cyber Counterintelligence", *5th International Workshop on ICT Uses In Warfare and the Safeguarding of Peace*, IEEE published conference proceedings, Pretoria, South Africa.

Gill, P. (2006) , "What is Intelligence Theory?' in Treverton, G F (et al), Toward a Theory of Intelligence – Workshop Report, RAND Cooperation, (http://www. rand. org/pubi/larf/ proceedings/2006 Rand – CF219.pdt).

Greenwald, A. G. (2012) "There Is Nothing So Theoretical as a Good Method", *Perspectives on Psychological Science*, Vol. 7, Nr 2.

Godson,R. (2001) *Dirty tricks or trump cards - U.S. covert action and counterintelligence*. Transaction Publishers, New Brunswick.

Heckman, K. E. et al (2015) *Cyber Denial, Deception and Counter-Deception: A Framework for Supporting Active Cyber Defense*. Springer, Switzerland.

Jaquire, V.J. (2017) *A Cyber Counterintelligence Maturity Model*, in-progress thesis towards a D.Com (Informatics) at the Academy of Computer Science and Software Engineering, University of Johannesburg.

Lee, R. M. (2014) 'Cyber Counterintelligence: From Theory to Practice.' Tripwire, blog series, part 4. Retrieved on 04/01/15 from http://www.tripwire.com/.../cyber-counterintelligence-from-theory-to-practice/

Prunckun, H (2012) *Counterintelligence: Theory and Practice*, Rowman & Little Publishers, Plymouth.

Molander, R.C., Riddile, A.S. & Wilson, P.A. (1996) *Strategic Information Warfare*, - *new face of war.* RAND Corporation, Santa Monica.

Oxford English Dictionary (2016) [online] http://0-www.oed.com.ujlink.uj.ac.za /view/ Entry/ 74161?redirectedFrom=Framework, accessed 13 November 2016.

Prunckun, H 2012. Counterintelligence: Theory and practice, Rowman & Littlefield Publishers, Plymouth, UK.

Stroz Friedberg (2017) *2017 Cybersecurity Predictions*, New York. , available at *https://www.strozfriedberg.com/press-release/cyber-risks-intensify-2017-increased-cyber-espionage-data-integrity-attacks-according-stroz-friedbergs-2017-cybersecurity-predictions-report/ce*,

The Economist (2015) "*Counter-intelligence techniques may help firms protect themselves against cyber-attacks", [online],* http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protectthemselves

Proceedings of the
17th European Conference on Cyber Warfare and Security
University of Oslo
Norway
28-29 June 2018

Edited by
Dr Audun Jøsang

acpi

A conference managed by ACPI, UK

Proceedings of the

17th European Conference on Cyber Warfare and Security ECCWS 2018

Hosted by
University of Oslo
Norway

28-29 June 2018

Edited by
Dr Audun Jøsang
University of Oslo, Norway

Review Process
Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy
ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:
http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academic-conferences-and-publishing-international-limited/

Conference Proceedings
The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

The Electronic version of the Conference Proceedings is available to download from DROPBOX http://tinyurl.com/ECCWS2018 Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.
The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-911218-86-9
E-Book ISSN: 2048-8610
Book version ISBN: 978-1-911218-85-2
Book Version ISSN: 2048-8602

Published by Academic Conferences and Publishing International Limited
Reading
UK
Tel: +44-118-972-4148
www.academic-conferences.org

Preface

These proceedings represent the work of researchers participating in the 17th European Conference on Cyber Warfare and Security (ECCWS) which is being hosted this year by University of Oslo, Norway on 28 - 29 June 2018.

ECCWS is a recognised event on the international research conferences calendar and provides a valuable platform for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the areas of Cyber Warfare and Security. It provides an important opportunity for researchers and practitioners to come together to share their experiences of researching in this varied and expanding field.

The first day will be opened with a keynote presentation by Siri Bromander who is part of the Threat Intelligence and Incident Response team at mnemonic, Oslo, Norway, will be speaking on *"Cyber Threat Intelligence (CTI)"*. Dr Olav Lysne of the Simula Research Laboratory, will then speak on the second day about *"Digital Vulnerability and International Interdependency"*.

With an initial submission of 137 abstracts, after the double blind, peer-review process there are 60 Academic Research papers, 10 PhD Research, 2 Masters Research, 2 Non-Academic and 1 Work in Progress paper published in these Conference Proceedings. These papers represent truly global research in the field, with contributions from Australia, Austria, Belgium, Finland, Germany, Greece, India, Ireland, Italy, Korea, Latvia, Lithuania, Malaysia, Netherlands, Norway, Portugal, Russia, South Africa, Sweden, Taiwan, USA, and UK.

We wish you a most interesting conference.

Dr Audun Jøsang
ECCWS Conference Chair
University of Oslo
Norway

A Selective Literature Review on Cyber Counterintelligence

Petrus Duvenage, Victor Jaquire and Sebastian von Solms

Centre for Cyber Security, Academy of Computer Science and Software Engineering, University of Johannesburg

duvenage@live.co.za
jaquire@gmail.com
basievs@uj.ac.za

Abstract: For state and non-state actors with sizable cyber interests, numerous breaches during this decade affirmed the necessity of having cyber counterintelligence (CCI) at the centre of cybersecurity efforts. Concurrent with the growing interest in CCI in corporate boardrooms and the corridors of governments, CCI is evolving from a field of academic enquiry to a distinctive academic sub-discipline. The growing body of CCI-focused literature clearly attests to this evolvement. A review of such literature not only has self-evident benefits for CCI's academic progression, but is also of use to the increasing number of practitioners specialising or interested in this area. Attempting a comprehensive literature review within the confines of a conference paper will be over-ambitious and, in the case of CCI, pre-mature. Therefore, the aim with this paper is to submit a tentative, selective review on CCI literature. This tentative 'bird's eye view' will hopefully provide a premise for progressing towards a more extensive and in-depth literature review.

Keywords: cyber counterintelligence, cyber warfare, cyber security, literature, theory, denial and deception.

1. Introduction

For state and non-state actors with sizable cyber interests, numerous breaches during this decade affirmed the necessity of having cyber counterintelligence (CCI) at the centre of cybersecurity efforts. Concurrent with the growing interest in CCI in corporate boardrooms and the corridors of governments, CCI is evolving from a field of academic enquiry to a distinctive academic sub-discipline. Attesting to the growing interest in CCI is the expanding body of peer-reviewed, academic contributions specifically focused on CCI. These contributions include numerous conference papers (e.g. Sigholm & Bang 2013; Jaquire & von Solms 2017*a-c*; Duvenage, von Solms & Corregidor 2016) and several completed post-graduate studies (e.g. Knowles 2013, Black 2014, Fieber 2015, Putnam 2015, Justiniano 2017, Jaquire 2018, Duvenage 2018). As we will illustrate in this paper, commercial literature on CCI has equally been growing steadily. A literature review not only has self-evident benefits for CCI's academic progression, but is also of use to the increasing number of practitioners specialising or interested in this area.

Attempting a comprehensive literature review within the confines of a conference paper will be over-ambitious and, in the case of CCI, pre-mature. Therefore, the aim with this paper is to submit a tentative, selective literature review on CCI. To this end the paper is structured as follows:

- Section 2 explains in more detail the purpose and benefits of a selective literature review on CCI.
- Section 3 defines the scope and explains the nature of the selected literature review.
- In Section 4, we present the literature review. This is done with reference to four literature categories, namely (1) peer-reviewed papers and articles, (2) masters and doctoral studies, (3) books and (4) other literature.
- We conclude in Section 5 with key findings and recommendations.

2. The purpose and benefits of a selective literature review for CCI

There are various types of reviews which serve different purposes (Grant & Booth 2009, Mallett *et al* 2012, Kim 2018). Some of these better known examples (of review types) include: argumentative- , integrative-, historical-, systematic-, methodological- and theoretical reviews. From these types, systematic reviews have for good reasons, been gaining prominence in academic circles (cf. Mallett *et al* 2012, Grant & Booth 2009). While systemic reviews hold various benefits, it is an exhaustive and extensive process.

Even for an academic sub-discipline as young as CCI, it would have been overambitious to endeavor a rigorous systematic review within the confines of a single conference paper. In a similar vein, we do not purport the

tentative overview presented in this paper to adhere to the requirements of one of the other review types. Instead, we follow a less formalistic and selective approach. Hopefully, this selective approach - which is further described in Section 3 - produces a review that has the following value:

- Highlight salient contributions to CCI which are of significant practical and/or academic importance.
- Provide some contours of the state of knowledge and the key directions of CCI research. Phrased
- Provide a 'scaffold' for identifying and positioning future research topics.
- Because our review deals with salient research done thus far, it could provide some insight into CCI's academic origin, emergence and development. As is the case with other academic subjects, a self-awareness of its origin and evolvement could contribute to consolidate CCI as a distinctive sub-discipline.
- Identify research projects/institutions focused on CCI and by so doing hopefully encouraging academic interaction in this field.

3. Qualifying the nature and scope of the selective CCI literature review

In the paper thus far, we emphasised the 'selective' nature and scope of the CCI literature review we are going to advance. For the review to be academic credible, we of course need to be clear on what the term 'selective' denotes. Our literature review is selective in that it limits its focus in the following three respects:

1) We firstly deem **'available literature'** as works in the **public domain**. Due cognisance is taken of the fact that state security structures internationally generate and possess CCI-relevant research and training material, of which some are unclassified, but not freely available. The same applies to some corporate entities and cybersecurity vendors which, for various considerations, do not openly share CCI material. For self-evident reasons, we categorically exclude from our review such material and, as far as possible, insights derived from such material. We secondly deem 'available literature' to refer to work published in **English**. Our search did consequently not cover untranslated CCI-research possibly published in other languages.

2) Our literature review is furthermore 'selective' in that we predominantly **focus on material which explicitly addresses CCI**. While overlapping themes (such as cyber denial and deception, insider threat mitigation, cyber intelligence and cyber threat intelligence) is important to CCI, a review of such literature would distract from our paper's aim. For purposes of this paper we define CCI (as the referent object of the literature overview) as that sub-discipline of counterintelligence (CI) " aimed at detecting, deterring, preventing, degrading, exploiting and neutralisation adversarial attempts to collect, alter or in any other way breach the C-I-A of valued information assets through cyber means." (Duvenage, von Solms & Corregedor 2016).

3) Thirdly, our literature review is selective in that it **does not purport be an inventory of all CCI-focused work within available literature**. Instead, we reflect on peer-reviewed, published academic work featured in selected platforms, namely: Scopus, EBSCO, IEEEE Explore, Springer Link, Google Scholar and Proquest.

4) Lastly, the literature review covers selected contributions **published up to 31 January 2018**.

In this section we qualified the literature overview's scope and approach. With these qualifications in mind, we now proceed with advancing the literature overview's structuring.

4. Selective CCI literature review

In order to appropriately structure our literature review, we considered the outcomes envisaged in Section 2. On the one hand, the conventional approach of dividing reviews per literature category (e.g. articles, papers, books) would arguably have been the best suited to plot existing, and to provide a scaffold for positioning future, CCI research.

On the other hand, a chronological literature review would be more effective to track CCI's academic origin and development. To strike a balance, we decided on an approach which incorporates a chronological thread

with literature type. Practically, this means that we structured the review per literature type. Since the bulk of academic work was produced per peer-reviewed articles and papers, we used this literature category (i.e. peer-reviewed articles and papers) to chronologically explain CCI's evolution. In tabulated format this can be depicted as follows:

<table>
<tr><th>Subsection</th><th>Literature category</th><th></th></tr>
<tr><td>4.1</td><td>Peer-reviewed articles and papers</td><td rowspan="4">← Subsection 4.1 provides the chronological thread and context

↓

Subsections 4.2 – 4.4 build on the chronology provided per Subsection 4.1.</td></tr>
<tr><td>4.2</td><td>Masters' and doctoral studies</td></tr>
<tr><td>4.3</td><td>Books</td></tr>
<tr><td>4.4</td><td>Other literature</td></tr>
</table>

Figure 1: Structural approach to the selective literature review on Cyber Counterintelligence

4.1 Peer-reviewed articles and papers

In this section, we will address some evolutional aspects of CCI, with specific reference to peer-review articles and papers. Although somewhat of an over-simplification, we divided CI's progression as a distinctive academic sub-discipline as follows:

- 4.1.1 Foundational phase (pre-2009)
- 4.1.2 Cyber Counterintelligence's emergence as an academic research theme (2009 -2012)
- 4.1.3 Cyber Counterintelligence crystallisation as a distinctive academic sub-discipline (2012 – present)

4.1.1 Foundational phase (pre-2009)

As far as we could surmise from available literature, the explicit term 'cyber counterintelligence' first emerged from the United States of America (USA) statutory security establishment during the early 2000's (cf. US 2004, French & Kim 2009). Prior to the 2000s, however, CCI existed *de facto* in the statutory security establishment of the USA and the security structures of some other countries. In this regard, French & Kim (2009) asserts that "cyber CI has existed *de facto* since the introduction of IT to intelligence, defense, and national security and has grown as FISs [Foreign Intelligence Services'] have embraced cyber tradecraft."

Concurrent with CCI's *de facto* existence in statutory security circles, a few sporadic academic articles in the 1980 and 1990s expounded key CCI notions - although without using the actual term 'cyber counterintelligence'. Such notions included the advocating of an integrated CI approach, which not only has defensive and offensive missions, but also synchronises human and technical resources. The earliest peer-reviewed article found in consulted literature referring to such application of a CI approach to the IT realm is contained in the electronic library of *the Institute of Electrical and Electronics Engineers (I.E.E.E.)*. This item, authored by Stone & Tucker (1988), is entitled 'Counterintelligence and Unified Technical Security Programs in Security Technology'. The authors expound effective CI as "unified multi-disciplinary concept" consisting of "proactive and defensive" missions". It is further argued that "advanced technology" is part of this multi-disciplinary entirety and serves both "proactive" (offensive) and defensive missions. While Stone & Tucker's (1988) paper centres on rectifying perceived deficiencies in the USA national CI endeavour thirty years ago, their key contentions on an integrated CI effort hold relevance up to this day.

In a related further contribution in the *I.E.E.E.* library, Stone and Bluitt (1993) further expanded on the idea of executing "advanced technological countermeasures" as part of "a pervasive counterintelligence (CI) mandate." Also Stone & Bluitt (1993) directed their paper specifically at the US statutory CI effort.

We found no articles or papers of direct CCI-relevance in consulted literature for the seven year period 1994 – 2001. The first peer-reviewed article we identified that specifically employs the term "cyber" in conjunction

with “counterintelligence” appeared in a 2002 issue of the *Journal of Information Warfare*. As suggested by the title of their article ‘Dominating the attacker: Use of intelligence and counterintelligence in cyber warfare’, Davey & Armstrong (2002) examine Intelligence and CI's role in augmenting cyber warfare. Cyberwarfare in turn, is firmly positioned as a subset of Information Warfare. By “employing intelligence and counterintelligence techniques that are superior to those of the attacker”, argue Davey & Armstrong (2002), the “cyberwarfare defender” is more likely to prevail. Davy & Armstrong (2002) urge a more “aggressive” posture which includes deception. One such example cited, is allowing the “attacker [to] gain access to information that is actually incorrect, thus providing incorrect intelligence.” In respect of CCI’s conceptual evolvement and especially CCI's relation to cyber warfare, the contribution of Davy & Armstrong (2002) represents a milestone.

As those by Stone & Tucker’s (1988) and Stone & Bluitt (1993), the work of Davey & Armstrong’s (2002) was part of CCI’s foundational phase which, if gauged by academic publications, was characterised by a few sporadic contributions. In as far as consulted literature go, no CCI-relevant publications appear for the next five years (2002-2008)

4.1.2 Cyber Counterintelligence’s emergence as a research theme (2009 -2012)

In contrast to the sporadic foundational phase, 2009 marked CCI’s emergence as a specific research theme attracting growing interest. In that year a seminal article appeared in the launch edition of the *National Intelligence Journal* (French & Kim 2009). This was the first academic publication (in consulted literature) to use the term "cyber counterintelligence". In this article, entitled ‘Acknowledging the revolution: The urgent need for cyber counterintelligence’, French & Kim (2009) called on the US intelligence community to move away move away from the notion that CCI is mostly part of “defensive Information Warfare”. Instead, French & Kim (2009) urged the USA to be more active and offensive in its approach to CCI. The work's relevance extends beyond the USA context. French & Kim (2009) explicitly define CCI, explain CCI’s missions within the context of CI, and offer various other insights on aspects useful to the further development within this field. Such aspects include the role of CCI in information warfare, critical infrastructure protection, and the CCI process and strategy.

The fact that we found no other peer-reviewed articles and papers in consulted literature for the 2009-2012 period, belies CCI’s emergence as a research theme for two reasons. Firstly, as we shall show in Sections 4.2 – 4.4 of this paper, a constant stream of CCI contributions emerged in other literature categories during this period. Secondly, the nature and extent of academic contributions on CCI from 2013 onward, strongly suggest that CCI attracted research interest in the preceding years (2009-2012).

4.1.3 Cyber Counterintelligence crystallisation as an academic sub-discipline (2013 – present)

As from 2013, the concurrent and consistent publication of numerous peer-reviewed papers and articles signalled CCI’s emergence as an academic sub-discipline with significant contributions from researchers in the USA, Sweden and South Africa.

The bulk of academic contributions from the USA stemmed from Utica College’s Master of Science Cybersecurity programme which offers CCI as a specialisation subject. This programme resulted in several “capstone project” papers (comparable to mini-dissertations in other countries) as well as a thesis, with CCI as a specific focus (Knowles 2013, Black 2014, Fieber 2015, Putnam 2015, Justiniano 2017). Since these contributions flow from a Master’s programme, they are later discussed in more detail in Section 4.2. Suffice to state here that this Utica research constitutes indispensable contributions to CCI on the conceptual, theoretical and praxis.

Albeit considerably more limited in scope than the research in the USA, papers delivered at two *I.E.E.E.* endorsed conferences in 2013 reflected growing interest also outside the USA. In August 2013, at the *European Intelligence & Security Informatics Conference* in Sweden, Sigholm and Bang’s (2013) submitted a paper entitled ‘Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats.’ Moving from a statutory military perspective, the paper is primarily aimed to advance a “comprehensive process that bridges the gap between the various actors involved in CCI”. Sigholm & Bang (2013) present this model to specifically configure the “offensive CCI attribution process”. The model essentially consists of an all-source information flow and analysis architecture to be employed for attribution purposes.

On the heels of Sigholm & Bang in 2013, Duvenage & von Solms (2013) presented 'The case for cyber counterintelligence' at the *5th International Conference on Adaptive Science and Technology* hosted in South Africa. The paper defines key CCI concepts and advance conceptual constructs which explain CCI and its relation to CI.

Duvenage & von Solms' (2013) paper formed parts of a dedicated CCI research project initiated at the University of Johannesburg's Cybersecurity Centre (UJCC) from which several other contributions would follow (University of Johannesburg, 2018). UJCC's website describes the project's aim as establishing CCI as a multi-disciplinary field of academic enquiry within the South African context (University of Johannesburg, 2018). To this end, the UJCC project pursues two complementary, yet parallel research streams, aimed respectively at

(1) Designing an overarching framework for conceptualising and explicating CCI as a distinctive academic field of enquiry, and:

(2) Develop a framework for a CCI maturity model for application by state and non-state actors within developing countries.

Building on Duvenage & von Solms (2013), UJCC's first research stream progressively advanced conceptual constructs to academically explain what CCI is, how it works and how it dovetails with other academic disciplines and theory. Such notional constructs, include a CCI-posture matrix model, CCI process model as well as a taxonomy of CCI tactics, tools, techniques and procedures (TTTPs). These notional constructs were submitted per the following peer-reviewed papers and a journal article:

- Duvenage & von Solms (2014) 'Putting counterintelligence in cyber counterintelligence' *in Published Proceedings of the 13th European Conference on Cyber Warfare and Security,* Piraeus, Greece.
- Duvenage & von Solms (2015) 'Cyber counterintelligence: Back to the future' in the *Journal of Information Warfare*.
- Duvenage, von Solms & Corregedor (2015) 'The cyber counterintelligence process – a conceptual overview and theoretical proposition' in the *Published Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, United Kingdom.
- Duvenage, Jaquire, & von Solms (2016) 'Conceptualising cyber counterintelligence – Two tentative building blocks' in the *Published Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, Germany.
- Duvenage, Sithole & von Solms (2017) 'A conceptual framework for cyber counterintelligence – theory that really matters!' in *Published Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland.

UJCC's second research stream, to recapitulate, aims to develop a CCI maturity model with emphasis on governments and non-state actors in emerging countries (University of Johannesburg, 2018). Peer-reviewed papers presented in this regard are as follow:

- Jaquire & von Solms (2017*a*) 'Towards a cyber counterintelligence maturity model' in the *Published Proceedings of the 12th International Conference on Cyber Warfare and Security*, Wright State University, Air Force Institute of Technology, Dayton (US).
- Jaquire & von Solms (2017*b*) 'Developing a cyber counterintelligence maturity model for developing countries' in the *Published Proceedings of the 2017 IST–Africa Conference*, Windhoek, Namibia.
- Jaquire & von Solms (2017*c*) 'Cultivating a cyber counterintelligence maturity model' in *Published Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland.

In this section we examined CCI's the academic evolvement at the hand of an overview of peer-reviewed articles and papers. In the next section, we explore masters and doctoral research focused on CCI.

4.2 Masters and doctoral studies

The search term 'cyber counterintelligence' (and variations thereof) showed numerous masters and doctoral studies of possible relevance to our CCI literature review. On closer analysis, however, most of these studies do not have CCI as a primary focus and CCI is not explored in depth. Instead, CCI is cursory referred to as part of the broader statutory CI mandate and mostly addressed within challenges faced by the USA Intelligence

community. Ferguson's (2012) thesis entitled *Increasing the effectiveness of U.S. counterintelligence: Domestic and international micro-restructuring initiatives to mitigate cyber espionage* serves as one such example.

Bucking this trend, Masters studies completed at Utica College from 2013 onwards delivered contributions which are pioneering and invaluable in respect of CCI's academic crystallisation and evolvement. As was noted earlier, these studies are mostly "capstone projects". While also conducted within the context of USA national interests and security, these studies have application and academic relevance wider than the USA. On the whole, important contributions are made to explicating CCI on the conceptual, theoretical and praxis levels. The following are some examples:

- In his research entitled *Applying computer network operations for offensive counterintelligence efforts*, Knowles (2013) identifies key aspects of Computer Network Operations (CNO). These aspects are then aligned with the broader intelligence and CI processes. In so doing "counterintelligence skills and techniques" are leveraged to "assimilate cyber activities" into an organisation's Intelligence endeavor.
- Effective CCI, argues Black (2014), is multidisciplinary and involves unique skill sets. In his thesis, entitled *The complexity of cyber counterintelligence training*, Black (2014) proceeds with identifying the implications thereof for CCI training. Black then advances two useful notional constructs namely (1) a CCI training model and (2) a CCI training proficiency path.
- As suggested by the research title, Putnam's (2015) *Digital mirrors casting cyber shadows - the confluence of cyber technology, psychology, and counterintelligence* emphasizes CCI's multidisciplinary nature. Putnam (2015) points out that a successful CI (and thus CCI) programme should consider the opportunities that technology presents as well as certain psychological "principles of persuasions" and motivation. The study details some offensive and defensive CCI applications of these opportunities and principles. Emphasis is placed in this regard on optimizing the CCI targeting and the recruitment processes.
- The interplay between practice and theory which characterises Utica College's research is reflected in Fieber's (2015) commendable contribution *The Iranian computer network operations threat to U.S. critical infrastructures.* Fieber (2015) analyses "the Iranian computer network operations (CNO) threat to U.S. critical infrastructures" and proceeds with recommending defensive measures to mitigate this threat. The paper culminates in a handy proposition on a phased, CCI process model "designed to mitigate conditions favorable to the attacker and restore the advantage to the organizational defenders."
- In a further outstanding and pioneering contribution, Justiniano (2017), with the research title *Advancing the capacity of a theatre special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone,* examines CCI's role in the USA military milieu while focused on the hybrid threats posed by Russia and the role of CCI in mitigating and engaging this threat, Justiniano's (2017) research is indispensable reading for examining CCI's role in hybrid warfare more generally. The study identifies critical CCI roles and skillsets before proceeding to propositions on integrating CCI with the USA Cyber Mission Assurance (C-MA) process in a manner supportive of Theater Special Operations Command (TSOC).

Although the bulk of post-graduate CCI studies in consulted literature originated from Utica College's Masters programme, the research project of the University of Johannesburg's Cyber Security Centre (UJCC) mentioned earlier, recently resulted in a Masters dissertation and Doctor's thesis focussing on CCI. These studies, which mirror UJCC's two CCI research streams (discussed in Subsection 4.1.3) are as follow:

- Jaquire (2018) *A framework for a cyber counterintelligence maturity model*, unpublished Doctor of Commerce thesis, University of Johannesburg.
- Duvenage (2018) *A conceptual framework for cyber counterintelligence*, unpublished Master of Commerce dissertation, University of Johannesburg.

In this subsection, we examined academic peer-reviewed literature on CCI. In the next section, we examine books published on the subject.

4.3 Books

The past two decades has seen an exponential rise in the number of books from reputable publishers dealing with aspects of cybersecurity. However, even outstanding books which address aspects of high relevance to CCI, make scant reference to CI and CCI. One such recent example is Heckman et al's (2015) *Cyber denial, deception and counter deception – A framework for supporting active cyber defense*. Despite this work arguably setting the standard for future works on cyber denial and deception in general, only four sentences in the entire book mentions the term 'counterintelligence' and there is no mention of 'cyber counterintelligence'.

In our search, we identified only one book which specifically and substantially focuses on CCI. This benchmark work was first published in 2012 with the title *Reverse deception – Organized cyber threat counter-exploitation* (Bodmer *et al.* 2012). Pitched as practicable guide for "IT security professionals", this book is also highly significant from an academic perspective. The book comprehensively examines the role of CCI in countering cyber threats through the engagement of hostile actors. In addition to CCI tactics, techniques and procedures (TTTPs), the authors explore CCI on a conceptual level. This includes postulations on CI missions, the CCI interface with CI and Intelligence, and other Intelligence fields. In nutshell, Bodmer *et al* (2012) is essential reading for any researcher interested in CCI.

4.4 Other literature

As with books, other forms of literature dealing with cybersecurity are continuing their sharp increase. Especially during the past eight years, there has been an upsurge in literature dealing with "threat intelligence", "cyber intelligence" and "cyber threat intelligence" (Duvenage, von Solms & Corregedor 2015). This is in part fuelled by cybersecurity vendors which are increasingly modelling their products and services on concepts derived from the state security and intelligence realms. In contrast to the bourgeoning discourse on for example threat intelligence and cyber intelligence, contributions to CCI are scarce but growing. In the main, contributions offer high-level explanations of what CCI is and point to the advantages that CCI practices could have in proactively addressing cyber insecurity. While 'commercial', such works nonetheless contribute to explicating CCI in concrete terms and, in some instances, are consequently also of academic value. Of such works, those by Lee (2014) and Bardin (2011), need to be singled out. The following examples of article headlines give a sense of the nature of contributions in commercial online literature:

- 'Cyber counter intelligence', in *Defense Tech Magazine* (Carrol 2009).
- 'Ten commandments of cyber counterintelligence' by Bardin (2011), first featured on the IDG News Service's online platform *CSO Online*.
- 'Offensive counter-intelligence and cyberwarfare – A paradigm shift in information security' on the *Information System Control and Audit Association (ISACA)* website (Farchi 2012).
- 'To thwart hackers, firms salting their servers with fake data', in *The Washington Post* (Nakashima 2013)
- 'Cyber counter-intelligence makes a difference', featured on the South African ITWeb website (von Solms 2014).
- 'Cyber counterintelligence: From theory to practice' by Lee (2014), first published on the website of the cybersecurity vendor *Tripwire*.
- 'Shifting paradigms: The case for cyber counter-intelligence', in *InformationWeek* (Firestone 2015).
- 'Counter-intelligence techniques may help firms protect themselves against cyber-attacks', published in *The Economist* (2015).

In this subsection, we cited some examples of commercial literature on CCI. In section to follow, we conclude the paper with key findings and suggestion on further research.

5. Conclusion

This paper advanced a tentative, selective literature review on CCI. This review shows CCI to have evolved, in less than a decade, from a research theme to a distinctive academic sub-discipline. In as far as consulted literature is concerned; the bulk of academic CCI research was conducted at Utica College and the University of Johannesburg. The nature and focus of these institutions' CCI research is inevitably influenced by the respective contexts of a super power and an emerging mid-income country. Perhaps as a result of these

differences, the work done is complementary in several respects. Collectively, the research covers diverse topics ranging from general theory and conceptualisation; to CCI training, process models, maturity frameworks as well as CCI's application to the military sphere.

Although it is gaining traction internationally, CCI is still in its academic infancy and thus offers numerous exciting research opportunities. There is, for example, especially a need for extensive research into CCI's interface with other academic disciplines. In addition, a comprehensive literature review, much broader in scope than this paper, will be an invaluable tool for CCI's progression.

Acknowledgment

The research presented in this paper forms part of a project at the Centre for Cyber Security (Academy for Computer Science and Software Engineering, University of Johannesburg) aimed at formalising CCI as a multi-disciplinary field of academic inquiry in the South African context. Those interested are invited to contact the authors and/or view more detail at http://adam.uj.ac.za/csi/CyberCounterintelligence.html.

References

Bardin, J. (2011) 'Ten commandments of cyber counterintelligence', CSO Magazine (online), accessed on 09/01/2013 at http://www.csoonline.com/article/2136458/identity-management/ten-commandments-of-cyber-counterintelligence.

Black, J.M. (2014). *The complexity of cyber counterintelligence training, unpublished* Master of Science dissertation, Utica College.

Boawn, D.L. (2014) *Cyber counterintelligence, defending the United States' information technology and communications critical infrastructure from Chinese threats*, unpublished master's dissertation, Utica College, New York, US.

Bodmer, S.A. et al. (2012) *Reverse deception – Organized cyber threat counter-exploitation*, McGraw-Hill, New York, US.

Carrol, J. (2009) 'Cyber counter intelligence in *Defense Tech*, accessed on 03/12/2012 at http://defensetech.org/2009/03/09/counter-cyber-intelligence/.

Davey, J. & Armstrong, H (2002) 'Dominating the attacker: Use of intelligence and counterintelligence in cyberwarfare' in *Journal of Information Warfare*, Vol. 2. Nr. 1.

Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2016) 'Conceptualising cyber counterintelligence – Two tentative building blocks' *in Published Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, Germany, June. Available at http://adam.uj.ac.za/csi/docs/ECCWS2016_DJVS_PDF.pdf

Duvenage, P.C., Sithole, T.G. & von Solms, S.H. (2017) 'A conceptual framework for cyber counterintelligence – Theory that really matters!' in *Published Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland, June. Available at http://adam.uj.ac.za/csi/docs/ECCWS_2017_DSV_Prof_MS.pdf

Duvenage, P.C. & von Solms. S.H. (2013) 'The case for cyber counterintelligence' in *Published Proceedings of the 5th International Workshop on ICT Uses in Warfare and the Safeguarding of Peace*, Institute of Electrical and Electronic Engineers (IEEE), Pretoria, South Africa, November.

Duvenage, P.C. & von Solms, S.H. (2014) 'Putting counterintelligence in cyber counterintelligence' in *Published Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece, July.

Duvenage, P.C. & von Solms. S.H. (2015) 'Cyber counterintelligence: Back to the future' in *Journal of Information Warfare*, 13(4):42–56. Available at http://adam.uj.ac.za/csi/docs/Journal%20of%20Information%20Warfare%20Duvenage_VonSolms%202015.pdf

Duvenage, P.C., von Solms, S.H. & Corregedor, M. (2015) 'The cyber counterintelligence process – A conceptual overview and theoretical proposition' in *Published Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK, July. Available at http://adam.uj.ac.za/csi/docs/ECCWS2015_Duvenage%20Von%20Solms%20Corregedor.pdf

Duvenage, P.C. (2018) *A conceptual framework for cyber counterintelligence*, unpublished Master of Commerce (Informatics) dissertation, University of Johannesburg

Farchi, J. (2012) 'Offensive counter-intelligence and cyberwarfare – A paradigm shift in information security' in *Information System Control and Audit Association (ISACA)*, accessed on 16/02/206 at http://www.isaca.org/Knowledge-Center/..../Post.aspx?List=ef7cbc6d%2D9997%2D4b62%2D96a4% .

Ferguson C. J. (2012) *Increasing the effectiveness of U.S. counterintelligence: Domestic and international micro-restructuring initiatives to mitigate cyberespionage*, unpublished master's dissertation, US Naval Postgraduate School, California, US.

Fieber, T. J. (2015) *The Iranian computer network operations threat to U.S. critical infrastructures*, Master of Science (capstone project), Utica College.

Firestone, A. (2015) 'Shifting paradigms: The case for cyber counter-intelligence' in *InformationWeek*, accessed at http://www.darkreading.com/operations/shifting-paradigms-the-case-for-cyber-counter-intelligence/a/d -id/1318929 .

French, G.S. & Kim, J. (2009) 'Acknowledging the revolution: The urgent need for cyber counterintelligence' in *National Intelligence Journal*, 1(1):71–90.

Heckman, K.E. et al. (2015) *Cyber denial, deception and counter deception – A framework for supporting active cyber defense*, Springer International Publishing, Cham, Switzerland.

Jaquire, V.J. (2018) *A framework for a cyber counterintelligence maturity model*, unpublished Doctor of Commerce (Informatics) thesis at the University of Johannesburg, Johannesburg, South Africa.

Jaquire, V.J. & von Solms, S.H. (2017*a*) 'Towards a cyber counterintelligence maturity model' in *Published Proceedings of the 12th International Conference on Cyber Warfare and Security*, Wright State University, Air Force Institute of Technology, Dayton, US, March.

Jaquire, V.J. & von Solms, S.H. (2017*b*) 'Developing a cyber counterintelligence maturity model for developing countries' in *Published Proceedings of the 2017 IST–Africa Conference, Windhoek,* Namibia, May–June.

Jaquire, V.J. & von Solms, S.H. (2017*c*) 'Cultivating a cyber counterintelligence maturity model' in Published Proceedings of the 16th European Conference on Cyber Warfare and Security, Dublin, Ireland, June.

Justiniano, JE . (2017) *Advancing the capacity of a theater special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone*, Master of Science (capstone project), Utica College.

Kim, J. S. (2018) *The Importance of Literature Review in Research Writing*. Available at https://owlcation.com /misc/literature_review

Knowles, J. A. (2013). *Applying computer network operations for offensive counterintelligence*, Master of Science (capstone project), Utica College.

Lee, R.M. (2014) 'Cyber counterintelligence: From theory to practice', *Tripwire* blog series (4), accessed on 2015/01/04 at http://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/ .

Mallett, R. et al (2012) 'The benefits and challenges of using systematic reviews in international development research' in the Journal *of Development Effectiveness, V*ol. 4, Issue 3.

Nakashima, E. (2013) 'To thwart hackers, firms salting there servers with fake data' in The Washington Post, accessed on 22/03/2013 at http://articles.washingtonpost.com/2013-01-02/world/36211654_1_ hackers-servers-contract-negotiations.

Putnam, R. T. (2015) *Digital mirrors casting cyber shadows - the confluence of cyber technology, psychology, and counterintelligence*, Master of Science (capstone project), Utica College.

Sigholm, J. & Bang, M. (2013) 'Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats' in Proceedings of the European Intelligence and Security Informatics Conference (EISIC), I.E.E.E, Uppsala, Sweden.

Stone, G.M. & Bluitt, K. (1993) 'Future law enforcement and internal security communications architecture employing advanced technologies', *IEEE Publication CH3372-0/93*, pp. 194 -202.

Stone, G.M. & Tucker R.S. (1988) 'Counterintelligence and unified technical security programs' in Security Technology, proceedings of the *IEEE International Carnahan Conference on Security Technology: Crime Countermeasures*, New York, October.

The Economist (2015) Counter-intelligence techniques may help firms protect themselves against cyber-attacks, accessed at http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protectthemselves.

United States of America (2004) Department of Defence, *Dictionary of Military and Associated Terms (12 April 2011 as amended through 7 October 2004)*. Available at http://www.bits.de/NRANEU/others/jp-doctrine/jp1_ 02%2804%29.pdf

University of Johannesburg (2018) *The Cyber Counterintelligence Project _Centre for Cybersecurity.* Available at http://adam.uj.ac.za/csi/CyberCounterintelligence.html

von Solms, S. H. (2014) 'Cyber counter-intelligence makes a difference' on *ITWeb*, first accessed on 11 November 2014 at http://www.itweb.co.za/index.php?option=com_content &view=article&id=134136

ANNEXURE H

Volume 17, Issue 4, Fall 2018
ISSN 1445-3312 (Printed Journal)
ISSN 1445-3347 (Online Journal)

JOURNAL OF INFORMATION WARFARE

Journal of Information Warfare

Journal of Information Warfare (JIW)

www.jinfowar.com

Scope

The journal has been created to provide a forum for discussion, information, and interaction between practitioners and academics in the broad discipline of information warfare/operations. It is of interest to professionals from the military, government, commerce, industry, education, and academy.

A full gambit of topics is covered—from the physical destruction of information systems to the psychological aspects of information use. The aim is to provide a definitive publication that makes available the latest thinking and research in the critical area of information warfare.

Submissions

The journal welcomes submissions. To learn more about preparing articles for submission, authors should visit the *JIW* website. Articles may be submitted to Diane Silver at dsilver@gbpts.com or Angel Linzy at alinzy@gbpts.com.

Authors' Responsibilities & Copyright

Authors are to ensure the accuracy of their papers. This journal does not accept any responsibility for statements made by authors in their written papers. Where relevant, authors are to ensure that the contents of their papers are cleared for publication, for example, by their employer, their client, the funding organization, and/or copyright owner of any material that is reproduced.

Subscriptions

The *Journal of Information Warfare* is published four times per year and is available both online and in hard copy.

Individual; **Individual, Student**; and **Corporate** subscriptions are available. For current pricing, see http://www.jinforwar.com/subscribe/.

Individual

A one-year subscription to the journal for individual subscribers. Both online-only and, online and print subscriptions are available.

Individual, Student

A one-year subscription to the journal for students. Evidence of full-time study must be provided. Both online-only and, online and print subscriptions are available.

Corporate

A one-year subscription to the journal for corporate/library subscribers. Both online-only and, online and print subscriptions are available. A single subscription covers unlimited use for a single campus/geographic location.

Note: Individual print copies of the journal are generally available for purchase only to subscribers and contributors.

All advertisements in this journal are printed free of charge as a service to readers.

Journal cover design, concept, and layout by Laima Croft.

Towards a Literature Review on Cyber Counterintelligence

PC Duvenage, VJ Jaquire, and SH von Solms

Centre for Cyber Security
Academy of Computer Science and Software Engineering
University of Johannesburg
Johannesburg, South Africa

E-mail: duvenage@live.co.za; jaquire@gmail.com; basievs@uj.ac.za

***Abstract**: For those connecting the dots, the threat landscape continues to affirm the necessity of having Cyber Counterintelligence (CCI) at the centre of cybersecurity efforts. Concurrent with the growing interest in CCI in corporate boardrooms and the corridors of governments, CCI is evolving from a field of academic enquiry to a distinctive academic sub-discipline. The growing body of CCI-focused literature clearly attests to this evolution. A review of such literature has self-evident academic and practical benefits. This article advances a tentative, selective review of CCI literature that demonstrates the need for a more extensive and in-depth appraisal.*

Keywords: *Cyber Counterintelligence, Cyber Warfare, Cyber Security, Literature, Theory, Denial and Deception*

Introduction

For state and non-state actors with sizable cyber interests, numerous breaches during this decade have affirmed the necessity of having Cyber Counterintelligence (CCI) at the centre of cybersecurity efforts (Prunckun 2018; Stech & Heckman 2018; *The Economist* 2015). Concurrent with the growing interest in CCI in corporate boardrooms and in the corridors of governments, CCI is evolving from a field of academic enquiry to a distinctive academic sub-discipline. Attesting to the growing interest in CCI is the expanding body of peer-reviewed, academic contributions specifically focused on CCI. These contributions include numerous conference papers (such as Sigholm & Bang 2013; Jaquire & von Solms 2017a-c; Duvenage, von Solms & Corregedor 2015) and several completed post-graduate studies (for example Knowles 2013; Black 2014; Fieber 2015; Putnam 2015; Justiniano 2017; Jaquire 2018; Duvenage 2018). As will be shown in this article, commercial literature on CCI has also been growing sharply in recent years.

A literature review not only has self-evident benefits for CCI's academic progress, but it will also be useful to the increasing number of practitioners specialising or interested in this area. Attempting a comprehensive and representative literature review within the confines of a single journal article will be over-ambitious. Moreover, in the case of a field as young as CCI, such an extensive review would arguably be pre-mature. Therefore, the article's aim is to submit a tentative, selective literature review on CCI. Such a pilot literature review reveals the need for a much more comprehensive and inclusive appraisal of CCI literature.

The rest of the article is structured as follows:

- First, the purpose and benefits of a selective literature review on CCI are discussed in more detail.
- Secondly, the scope and the nature of the selective literature review are defined.
- Subsequently, the literature review is presented with reference to four literature categories, namely (1) peer-reviewed papers and articles, (2) masters' and doctoral studies, (3) books and (4) other literature.
- Finally, the conclusion submits key findings and observations regarding the way forward.

The Purpose and Benefits of a Selective Literature Review on CCI

Within academic research in general, there are various types of literature reviews which serve different purposes (Grant & Booth 2009; Mallett *et al.* 2012; Kim 2018). Some better-known examples (of review types) include: argumentative-, integrative-, historical-, systematic-, methodological- and theoretical reviews. From these types, systematic reviews have, for good reasons, been gaining prominence in academic circles (Mallett *et al*. 2012; Grant & Booth 2009). While a systemic review has many benefits, its compilation is an exhaustive and extensive process.

As suggested earlier, even for an academic sub-discipline as young as CCI, it would have been over-ambitious at this stage to endeavour to create a rigorous systematic review of CCI literature and to present the outcome thereof in a single journal article. In a similar vein, the tentative overview presented in this paper does not purport to adhere to the requirements of one of the other review types cited above. Instead, the article follows a less formalistic and selective approach in its review of CCI literature. This selective approach—further scoped and qualified in the next section ('Qualifying the Nature and Scope of the Selective CCI Literature Review')—provides a number of benefits:

- It highlights salient contributions to CCI that are of significant practical and/or academic importance;
- It provides some contours of the state of knowledge and the key directions of CCI research;
- It establishes a 'scaffold' for identifying and positioning future research topics;
- It provides a premise for a more comprehensive, systematic CCI literature survey;
- Because it deals with salient research done thus far, it offers an insight into CCI's academic origin, emergence, and development. As is the case with other academic subjects, such a self-awareness of origin and evolution could contribute to consolidating CCI as a distinctive sub-discipline; and
- It identifies research projects/institutions focused on CCI and, by so doing, encourages academic interaction in this field.

Qualifying the Nature and Scope of the Selective CCI Literature Review

This article has thus far emphasised the 'selective' nature and scope of the CCI literature review to be advanced. For the review to be academically credible, the meaning of the word 'selective' needs to be clarified. The review of literature advanced in this article is selective in that it limits its focus in the following five respects:

1) 'Available literature' is deemed as works in the **public domain**. Due cognisance is taken of the fact that state security structures internationally generate and possess CCI-relevant research and training material, some of which is unclassified but not

freely available. The same applies to some corporate entities and cybersecurity vendors that, for various reasons, do not openly share CCI material. Such material is categorically excluded from this review.

2) 'Available literature' is secondly deemed as referring to work published in **English**. The search which informed the review did not cover untranslated CCI-research possibly published in other languages.
3) The literature review is furthermore 'selective' in that it predominantly focuses on material which **explicitly addresses CCI**. While overlapping themes (such as cyber denial and deception, insider threat mitigation, cyber intelligence, and cyber threat intelligence) are important to CCI, a review of such literature would distract from the article's aim. For purposes of the article, CCI—which constitutes the literature overview's referent object—is defined as that sub-discipline of counterintelligence (CI) "aimed at detecting, deterring, preventing, degrading, exploiting and neutralis[ing] adversarial attempts to collect, alter or in any other way breach the C-I-A of valued information assets through cyber means" (Duvenage, von Solms & Corregedor 2015).
4) The literature review is selective in that it **does not purport be an inventory** of all CCI-focused work. Instead, in terms of academic works, the review reflects on peer-reviewed, published work featured in selected platforms, namely Scopus, EBSCO, Institute of Electrical and Electronics Engineers (IEEE), Explore, Springer Link, Google Scholar, and Proquest.
5) Lastly, the literature review only covers selected contributions **published as of 30 April 2018**.

Moving from the foregoing calibration of the CCI literature overview's selective scope, the next section explains the structural approach to be followed.

Structural Approach to the Selective CCI Literature Review

A literature review should, of course, be structured in a manner optimally achieving its aim and benefits. Given this literature review's earlier discussed aim and benefits, structuring the review per either (a) literature category or (b) chronology of publication was considered. On the one hand, the conventional approach of dividing reviews per literature category (such as articles, masters' and doctoral studies, books) would arguably have been the best suited to plot existing and to provide a scaffold for positioning future CCI research. On the other hand, a chronological literature review would be more effective to convey CCI's academic origin and development. To draw on the advantages both these styles offer, this article opted for a hybrid approach which incorporates a chronological thread with literature type. Practically, this means that the review overall is structured per the literature categories, namely peer-reviewed articles and papers, masters' and doctoral studies, books, and other literature. However, since the bulk of CCI academic work was produced per peer-reviewed articles and papers, this literature category (peer-reviewed articles and papers) is presented chronologically in order to convey CCI's origin and evolution.

This hybrid structural approach to the selective CCI literature review is depicted in **Figure 1,** below.

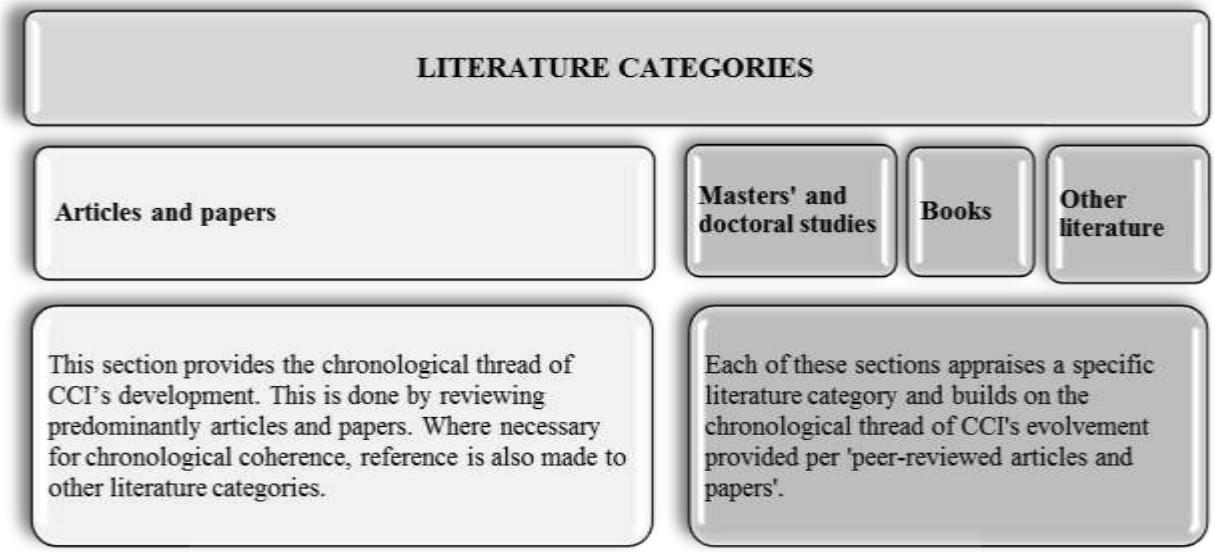


Figure 1: Structural approach to the selective literature review on Cyber Counterintelligence

Peer-Reviewed Articles and Papers

In line with **Figure 1**, this section enumerates CCI's evolution with specific reference to peer-reviewed articles and papers. Although somewhat of an over-simplification, CCI's progression as a distinctive academic sub-discipline consists of the following phases:

- Foundational phase (pre-2009),
- Phase in which Cyber Counterintelligence's emerged as an academic research theme (2009-2012),
- Current stage in which Cyber Counterintelligence crystallised into a distinctive academic sub-discipline (2012-present).

Foundational phase (pre-20

As far as could be surmised from available literature, the explicit term 'Cyber Counterintelligence' first emerged in the United States of America (U.S.) statutory security establishment during the early 2000s (see U.S. 2004; French & Kim 2009). Prior to the 2000s, however, CCI was practiced in the statutory security establishment of the U.S. and the security structures of some other countries. In this regard, French and Kim (2009) rightly assert that "cyber CI has existed *de facto* since the introduction of IT to intelligence, defence, and national security and has grown as FISs [Foreign Intelligence Services] have embraced cyber tradecraft".

Concurrent with CCI's *de facto* existence in statutory security circles, a few sporadic academic articles in the 1980s and 1990s expounded key CCI notions—although without using the actual term 'Cyber Counterintelligence'. Such notions included advocating for an integrated CI approach, which not only has defensive and offensive missions, but which also synchronises human and technical resources. The earliest peer-reviewed article found in consulted literature referring to such application of a CI approach to the IT realm is contained in the electronic library of the Institute of Electrical and Electronics Engineers (IEEE). This item, authored by Stone and Tucker (1988), is entitled 'Counterintelligence and unified technical security programs in security technology'. The authors expound effective CI as a "unified multi-disciplinary concept" consisting of "proactive and defensive" missions. Stone and Tucker (1988) further argue that "advanced technology" is part of the multi-disciplinary

CI entirety and thus serves both "proactive" (offensive) and defensive missions. While Stone and Tucker's (1988) paper centres on rectifying perceived deficiencies in the U.S. national CI endeavour thirty years ago, their key contentions regarding an integrated CI effort are still relevant today.

In a related further contribution in the IEEE library, Stone and Bluitt (1993) further expanded on the idea of executing "advanced technological countermeasures" as part of "a pervasive counterintelligence (CI) mandate". Also, Stone and Bluitt (1993) directed their paper specifically at the U.S. statutory CI effort.

No articles or papers of direct CCI-relevance were found in consulted literature for the seven-year period from 1994 through 2001. The first peer-reviewed article that specifically employs the term "cyber" in conjunction with "counterintelligence" appeared in a 2002 issue of the *Journal of Information Warfare*. As suggested by the title of the article, 'Dominating the attacker: Use of intelligence and counterintelligence in cyber warfare', Davey and Armstrong (2002) examined Intelligence and CI's role in augmenting cyber warfare. Cyberwarfare, in turn, is firmly positioned as a subset of Information Warfare. By "employing intelligence and counterintelligence techniques that are superior to those of the attacker", argue Davey and Armstrong (2002), the "cyberwarfare defender" is more likely to prevail. Davy and Armstrong (2002) urge a more "aggressive" posture that includes deception. One such example cited includes allowing the "attacker [to] gain access to information that is actually incorrect, thus providing incorrect intelligence". In respect to CCI's conceptual evolution and especially CCI's relation to cyber warfare, the contribution of Davy and Armstrong (2002) represents a milestone.

Like the work of Stone and Tucker (1988) and Stone and Bluitt (1993), Davey and Armstrong's 2002 article was part of CCI's foundational phase which, if gauged by academic publications, was characterised by only a few sporadic contributions. In as far as consulted literature goes, no CCI-relevant publications appear for the next five years (2002-2008).

Cyber Counterintelligence's emergence as a research theme (2009 -2012)

Following a sporadic foundational phase, 2009 marked CCI's emergence as a specific research theme attracting growing interest. In that year, a seminal article appeared in the launch edition of the *National Intelligence Journal* (French & Kim 2009). This was the first academic publication (in consulted literature) to use the term "Cyber Counterintelligence". In 'Acknowledging the revolution: The urgent need for Cyber Counterintelligence', French and Kim (2009) call on the U.S. intelligence community to move away from the notion that CCI is mostly part of "defensive Information Warfare". Instead, French and Kim (2009) urge the U.S. to be more active and offensive in its approach to CCI. The work's relevance extends beyond the U.S. context. French and Kim (2009) explicitly define CCI, explain CCI's missions within the context of CI, and offer various other insights on aspects useful to the further development within this field. Such aspects include the role of CCI in information warfare, critical infrastructure protection, and the CCI process and strategy.

No other peer-reviewed articles and papers were found in consulted literature for the 2009 through 2012 period. It must, however, be emphasised strongly that the absence of academic articles on CCI in consulted literature belies CCI's emergence as a research theme for three reasons. First, there were several CCI contributions during this period in other literature categories (see subsequent section entitled 'Other literature') and in publications not covered by this article's selective review. (See, for example, U.S. Naval War College 2018,

"Counterintelligence: Cyber Threat".) Thirdly, the nature and extent of academic contributions regarding CCI from 2013 onward strongly suggest that CCI attracted research interest in the preceding years (2009-2012). Phrased differently, research was done in the 2009-2012 timeframe, but the fruits thereof, in the main, are only reflected from 2013 onward.

Cyber Counterintelligence crystallisation as an academic sub-discipline (2013-present)

From 2013, a consistent stream of peer-reviewed papers and articles signalled CCI's emergence as an academic sub-discipline with significant contributions in English from researchers in the U.S., Sweden, and South Africa.

The bulk of academic contributions from the U.S. stemmed from Utica College's Master of Science Cybersecurity programme that offers CCI as a specialisation subject. This programme resulted in several "capstone project" papers (comparable to mini-dissertations in other countries) as well as a thesis, with CCI as a specific focus (Knowles 2013; Black 2014; Fieber 2015; Putnam 2015; Justiniano 2017). Since these contributions flow from a master's programme, they are discussed in more detail in a later section, which focuses on masters' and doctoral studies). Suffice to state here that this Utica research constitutes indispensable contributions to CCI on the conceptual, theoretical, and praxis levels.

Also, in recent years in the U.S., the concept of CCI has attracted interest from researchers at the Mitre Corporation. Branching out from their leading research on denial and deception in active cyber defence, the "applications of cyber counterintelligence" to "cyber defense" was subsequently examined (Heckman *et al*. 2015; Stech & Heckman 2018). Flowing from this research, Stech and Heckman (2018) contribute a book chapter, which is a undoubtedly one of the most incisive and significant works on CCI to date. (This contribution is discussed in more detail under 'Books'.)

Albeit considerably more limited in scope than the research in the U.S., papers delivered at two IEEE-endorsed conferences in 2013 reflected growing interest also outside the U.S. In August 2013, at the European Intelligence & Security Informatics Conference in Sweden, Sigholm and Bang (2013) submitted a paper entitled 'Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats'. Coming from a statutory military perspective, the paper is primarily aimed to advance a "comprehensive process that bridges the gap between the various actors involved in CCI". Sigholm and Bang (2013) present this model to specifically configure the "offensive CCI attribution process". The model essentially consists of all-source information flow and analysis architecture to be employed for attribution purposes.

On the heels of Sigholm & Bang in 2013, Duvenage & von Solms (2013) presented 'The case for cyber counterintelligence' at the 5th International Conference on Adaptive Science and Technology in South Africa. The paper defines key CCI concepts and advances conceptual constructs which explain CCI and its relation to CI.

Duvenage and von Solms' (2013) paper formed part of a dedicated CCI research project initiated at the University of Johannesburg's Cybersecurity Centre (UJCC) from which several other contributions would follow (University of Johannesburg 2018). UJCC's website describes the project's aim as establishing CCI as a multi-disciplinary field of academic enquiry within the South African context (University of Johannesburg 2018). To this end, the

UJCC project pursues two complementary yet parallel research streams, aimed respectively at:

1) Designing an overarching framework for conceptualising and explicating CCI as a distinctive academic field of enquiry, and;
2) developing a framework for a CCI maturity model for application by state and non-state actors within developing countries.

Building on Duvenage and von Solms' 2013 contribution, UJCC's first research stream progressively advanced conceptual constructs to explain (in an academic context) what CCI is, how it works, and how it dovetails with other academic disciplines and theory. Such notional constructs include a CCI-posture matrix model and a CCI process model, as well as a taxonomy of CCI Tactics, Tools, Techniques, and Procedures (TTTPs). These notional constructs were submitted per the following peer-reviewed papers and a journal article:

- Duvenage and von Solms (2014), 'Putting counterintelligence in cyber counterintelligence' in *Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece.
- Duvenage and von Solms (2015), 'Cyber counterintelligence: Back to the future' in the *Journal of Information Warfare*.
- Duvenage, von Solms, and Corregedor (2015), 'The cyber counterintelligence process – a conceptual overview and theoretical proposition' in *Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK.
- Duvenage, Jaquire, and von Solms (2016), 'Conceptualising cyber counterintelligence – two tentative building blocks' in *Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, DE.
- Duvenage, Sithole, and von Solms (2017), 'A conceptual framework for cyber counterintelligence—theory that really matters!', *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland.

UJCC's second research stream, to recapitulate, aims to develop a CCI maturity model with emphasis on governments and non-state actors in emerging countries (University of Johannesburg 2018). Peer-reviewed papers presented in this regard are as follow:

- Jaquire and von Solms (2017a), 'Towards a cyber counterintelligence maturity model', in *Proceedings of the 12th International Conference on Cyber Warfare and Security*, Wright State University, Air Force Institute of Technology, Dayton, OH, U.S.
- Jaquire and von Solms (2017b), 'Developing a cyber counterintelligence maturity model for developing countries' in *Proceedings of the 2017 IST–Africa Conference*, Windhoek, Namibia.
- Jaquire and von Solms (2017c), 'Cultivating a cyber counterintelligence maturity model' in *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland.

This section examined CCI's academic evolution via an overview of peer-reviewed articles and papers. The next section explores contributions to the field in the form of masters' and doctoral research.

Masters' and Doctoral Studies

The search term 'Cyber Counterintelligence' (and variations thereof) showed numerous masters' and doctoral studies of possible relevance to a CCI literature review. On closer analysis, however, most of these studies do not have CCI as a primary focus, and CCI is not explored in depth. Instead, CCI is cursorily referred to as part of the broader statutory CI mandate and mostly addressed within challenges faced by the U.S. Intelligence community. Ferguson's (2012) thesis entitled *Increasing the effectiveness of U.S. counterintelligence: Domestic and international micro-restructuring initiatives to mitigate cyber espionage* serves as one such example.

Bucking this trend, masters' studies completed at Utica College from 2013 onwards delivered contributions that are pioneering and invaluable with respect to the academic crystallisation and evolution of CCI. As was noted earlier, these studies are mostly "capstone projects". Also conducted within the context of U.S. national interests and security, these studies have much broader application and academic relevance than just in the U.S. Overall, important contributions have been made to explicating CCI on the conceptual, theoretical, and praxis levels. The following are some examples:

- In his research entitled *Applying computer network operations for offensive counterintelligence efforts,* Knowles (2013) identifies key aspects of Computer Network Operations (CNO). These aspects are then aligned with the broader intelligence and CI processes. In so doing, "counterintelligence skills and techniques" are leveraged to "assimilate cyber activities" into an organisation's Intelligence endeavour.
- Effective CCI, argues Black (2014), is multidisciplinary and involves unique skill sets. In his thesis, entitled *The complexity of cyber counterintelligence training*, Black proceeds with identifying the implications thereof for CCI training. Black then advances two useful notional constructs, namely (1) a CCI training model and (2) a CCI training proficiency path.
- As suggested by the research title, Putnam's (2015) *Digital mirrors casting cyber shadows - The confluence of cyber technology, psychology, and counterintelligence* emphasises CCI's multidisciplinary nature. Putnam points out that a successful CI (and thus CCI) programme should consider the opportunities that technology presents as well as certain psychological "principles of persuasions" and motivation. The study details some offensive and defensive CCI applications of these opportunities and principles. Emphasis is placed in this regard on optimizing the CCI targeting and the recruitment processes.
- The interplay between practice and theory which characterises Utica College's research is reflected in Fieber's (2015) commendable contribution: *The Iranian computer network operations threat to U.S. critical infrastructures.* Fieber analyses "the Iranian computer network operations (CNO) threat to U.S. critical infrastructures" and proceeds with recommending defensive measures to mitigate this threat. The paper culminates in a handy proposition on a phased, CCI process model "designed to mitigate conditions favorable to the attacker and restore the advantage to the organizational defenders" (Fieber 2015).
- Justiniano's 2017 outstanding and pioneering contribution, entitled *Advancing the capacity of a theatre special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone,* examines CCI's role in the U.S. military milieu with a focus on the hybrid threats posed by Russia and the role of CCI in mitigating and engaging this threat. Justiniano's (2017) research is indispensable reading for

examining CCI's role in hybrid warfare more generally. The study identifies critical CCI roles and skillsets before proceeding to propositions on integrating CCI with the U.S. "Cyber Mission Assurance (C-MA)" process in a manner supportive of "Theater Special Operations Command (TSOC)".

Although the bulk of post-graduate CCI studies in consulted literature originated from Utica College's Master's programme, the research project of the University of Johannesburg's Cyber Security Centre (UJCC), mentioned earlier, recently resulted in a master's dissertation and doctoral thesis focussing on CCI. These studies, which mirror UJCC's two CCI research streams (discussed in the article's previous section), are as follow:

- Jaquire (2018) *A framework for a cyber counterintelligence maturity model*, Doctor of Commerce thesis, University of Johannesburg, South Africa.
- Duvenage (2018) *A conceptual framework for cyber counterintelligence*, Master of Commerce dissertation, University of Johannesburg, South Africa.

The preceding two sections focused on academic, peer-reviewed literature—which ranges from papers and articles to masters' and doctoral studies. In the next section, books published on CCI are reviewed.

Books

The past two decades has seen an exponential rise in the number of books from reputable publishers dealing with aspects of cybersecurity. However, until very recently, even outstanding books that address aspects of high relevance to CCI make scant reference to CI and CCI. One such example is Heckman *et al.*'s (2015) *Cyber denial, deception and counter deception – A framework for supporting active cyber defense*. Despite the likelihood that this work sets the standard for future works on cyber denial and deception in general, only four sentences in the entire book mention the term 'counterintelligence', and there is no mention of 'Cyber Counterintelligence'.

The first book identified by the survey conducted for this article that has a significant CCI focus was published in 2012 with the title *Reverse deception—Organized cyber threat counter-exploitation* (Bodmer *et al.* 2012). Pitched as a practical guide for "IT security professionals", this text is highly significant from an academic perspective. The book comprehensively examines the role of CCI in countering cyber threats through the engagement of hostile actors. In addition to describing CCI Tactics, Techniques, and Procedures (TTPs), the authors also explore CCI on a conceptual level. This includes postulations on CI missions as well as CCI's interface with CI and other Intelligence fields. In nutshell, Bodmer *et al.* (2012) is essential reading for any researcher interested in CCI.

The next book to include a pertinent and significant CCI focus appeared under the editorship of Prunckun (2018) and is entitled *Cyber weaponry: Issues and implications of digital arms*. While the book has several chapters useful to CCI, Chapter Two is specifically dedicated to CCI. Under the title, 'Human Nature and Cyber Weaponry: Use of Denial and Deception in Cyber Counterintelligence', Stech and Heckman (2018) make a masterful contribution which anyone serious about CCI should consult. The chapter's primary aim is to advance a "cyber counterintelligence framework in active cyber defences". This system is "referred to as the cyber deception chain, to mitigate cyber spy actions within the cyber espionage 'kill chain'" (Stech & Heckman 2018). To lay a foundation for their CCI framework, Stech and Heckman explain the need for CCI. They proceed by appraising CI definitions, status, and existing

frameworks with a view on application to active defense in CCI. The text also observes the existing body of CCI academic research. Proceeding from this basis, Stech and Heckman (2018) present their CCI framework for "active cyber defense". This framework applies and synergises earlier postulations by Duvenage and von Solms (2014) and Prunkun (2014). Stech & Heckman (2018) demonstrate the framework's application by means of a hypothetical case involving the North Atlantic Treaty Organisation (NATO) and the Russian Federation.

Other Literature

In the past eight years, there has been an upsurge in literature dealing with "threat intelligence", "cyber intelligence", and "cyber threat intelligence" (Duvenage, von Solms & Corregedor 2015). Cybersecurity vendors, who are increasingly modelling their products and services on concepts derived from the state security and intelligence realms, in part fuel this upsurge. In contrast to the bourgeoning discourse on, for example, 'threat intelligence' and 'cyber intelligence', contributions to CCI are more limited but are growing. In the main, contributions offer high-level explanations of what CCI is and point to the advantages that CCI practices could have in proactively addressing cyber insecurity. While 'commercial', such works nonetheless contribute to explicating CCI in concrete terms and, in some instances, are consequently also of academic value. In this regard, works by Bardin (2011), Farchi (2012), and Lee (2014) can be singled out.

The following examples of article headlines give a sense of the nature of contributions in commercial online literature:

- 'Cyber counter intelligence', in *Defense Tech Magazine* (Carrol 2009);
- 'Ten commandments of cyber counterintelligence' by Bardin (2011), first featured on the IDG News Service's online platform *CSO Online*;
- 'Offensive counter-intelligence and cyberwarfare—A paradigm shift in information security' on the *Information System Control and Audit Association (ISACA)* website (Farchi 2012);
- 'To thwart hackers, firms salting their servers with fake data', in *The Washington Post* (Nakashima 2013);
- 'Cyber counter-intelligence makes a difference', featured on the South African ITWeb website (von Solms 2014);
- 'Cyber counterintelligence: From theory to practice' by Lee (2014), first published on the website of the cybersecurity vendor *Tripwire*;
- 'Shifting paradigms: The case for cyber counter-intelligence', in *InformationWeek* (Firestone 2015); and
- 'Counter-intelligence techniques may help firms protect themselves against cyber-attacks', published in *The Economist* (2015).

While videos are not typically included in literature reviews, CCI's incipient status as well as the merits of a contribution in video format, warrant an exception. This video covers a presentation by Evron (2014), then chairman of the board of the Israeli Computer Emergency Response Team (CERT). This high-level presentation provides a concise, yet incisive and conceptually sharp overview of key CCI fundamentals.

This section reviewed some examples of other literature on CCI. In the section that follows, the article concludes with findings and observations regarding the way forward.

Conclusion

This article advanced a tentative, selective literature review on CCI. This review shows CCI to have evolved, in less than a decade, from a research theme to a distinctive academic sub-discipline. As far as consulted literature is concerned, the bulk of peer-reviewed academic CCI research—documented in papers, articles and post-graduate studies—was conducted at Utica College (U.S.) and the University of Johannesburg (South Africa). The nature and focus of these institutions' CCI research are inevitably influenced by the respective contexts of a super power (U.S.) and an emerging mid-income country (South Africa). Perhaps because of these differences, the work done is complementary in several respects. Collectively, the research covers diverse topics ranging from general theory and conceptualisation; to CCI training, process models, and maturity frameworks, as well as CCI's application in the military domain. With respect to books and other literature categories, outstanding contributions include works by Stech and Heckman (2018), Evron (2014), Bardin (2011), Farchi (2012), and Lee (2014).

Although CCI is gaining traction internationally, this literature review shows that it is still in its academic infancy and, thus, offers numerous exciting research opportunities. A comprehensive literature review, much broader in scope than this article, would be an invaluable tool for CCI's progression. Such a review would have to cover research in languages other than English and in numerous other databases. Initial research on a comprehensive literature review is being conducted and is already delivering promising results. Those interested in cooperating in this venture are invited to contact the article authors.

Acknowledgments

The research presented in this article forms part of a project at the University of Johannesburg's Centre for Cyber Security. More detail can be viewed at <http://adam.uj.ac.za/csi/CyberCounter intelligence.html>.

References

Bardin, J 2011 'Ten commandments of cyber counterintelligence', *CSO Magazine*, 21 June, viewed 7 May 2015, <http://www.csoonline.com/article/2136458/identity-management/ten-commandments-of-cyber-counterintelligence>.

Black J M 2014, *The complexity of cyber counterintelligence training*, Master of Science dissertation, Utica College, New York, US.

Bodmer, S, Kilger, M, Carpenter, G & Jones, J 2012, *Reverse deception—Organized cyber threat counter-exploitation*, McGraw-Hill, New York, US.

Carrol, J 2009, 'Cyber counter intelligence' *Defense Tech*, 9 March, viewed 10 October 2014, <https://www.military.com/defensetech/2009/03/09/counter-cyber-intelligence>.

Davey, J & Armstrong, H 2002, 'Dominating the attacker: Use of intelligence and counterintelligence in cyberwarfare', *Journal of Information Warfare*, vol. 2, no. 1, pp. 23-31.

Duvenage, PC, Jaquire, VJ, & von Solms, SH 2016, 'Conceptualising cyber counterintelligence—Two tentative building blocks', *Proceedings of the 15th European Conference on Cyber Warfare and Security*, R Koch & G Rodosek (eds), Munich, DE,

viewed 2 November 2018, <http://adam.uj.ac. za/csi/docs/ECCWS2016_DJVS_PDF.pdf>, pp. 93-103.

Duvenage, PC, Sithole, TG & von Solms, SH 2017, 'A conceptual framework for cyber counterintelligence—theory that really matters!', M Scanlon & L Neihn-An (eds), *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland, viewed 11 December 2018, <http://adam.uj.ac.za/csi/docs/ECCWS_2017_DSV_Prof_MS.pdf>, pp.109-19.

Duvenage, PC & von Solms SH 2013, 'The case for cyber counterintelligence', *Proceedings of the 5th international conference on Adaptive Science and Technology*, IEEE, T Fogwill (ed.), Pretoria, South Africa, viewed 7 August 2014, <https://ieeexplore.ieee.org/document/6707493/>, pp. 1-8.

——2014, 'Putting counterintelligence in cyber counterintelligence', A Liaropoulos & GA Tsihrintzis (eds), *Published Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece, pp. 70-9.

——2015, 'Cyber counterintelligence: Back to the future', *Journal of Information Warfare*, vol. 13, no. 4, pp. 42-56.

Duvenage, PC, von Solms, SH & Corregedor, M 2015, 'The cyber counterintelligence process—A conceptual overview and theoretical proposition', *Proceedings of the 14th European Conference on Cyber Warfare and Security*, N Abouzakhar (ed.), Hatfield, UK, viewed 2 September 2018, <http://adam.uj.ac.za/csi/docs/ECCWS2015_Duvenage %20Von%20Solms%20Corregedor.pdf >, pp. 42-51.

Duvenage, PC 2018, *A conceptual framework for cyber counterintelligence*, Master of Commerce (Informatics) dissertation, University of Johannesburg, South Africa.

The Economist 2015, *Counter-intelligence techniques may help firms protect themselves against cyber-attacks*, viewed 24 May 2016, <http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protectthemselves>.

Evron, G 2014, *Cyber Counter Intelligence: An attacker-based approach*, Honeynet Project Workshop, Warsaw, Poland, May 2014, viewed 7 October 2017, <https://www.youtube.com/watch?v=lJC3c-jMALU>.

Farchi, J 2012, 'Offensive counter-intelligence and cyberwarfare—A paradigm shift in information security', *Information System Control and Audit Association (ISACA)—Blog*, viewed 16 February 2016, <http://www.isaca.org/Knowledge-Center/..../Post.aspx?List=ef7cbc6d%2D9997%2D4b62%2D96a4% >.

Ferguson CJ 2012, *Increasing the effectiveness of U.S. counterintelligence: Domestic and international micro-restructuring initiatives to mitigate cyberespionage*, Master's dissertation, US Naval Postgraduate School, Monterey, California, US.

Fieber, TJ 2015, *The Iranian computer network operations threat to U.S. critical infrastructures*, Master of Science (capstone project), Utica College, New York, US.

Firestone, A 2015, 'Shifting paradigms: The case for cyber counter-intelligence', *InformationWeek*, 2 April, viewed 7 July 2016, <http://www.darkreading.com/operations/shifting-paradigms-the-case-for-cyber-counter-intelligence/a/d-id/1318929 >.

French, GS & Kim, J 2009, 'Acknowledging the revolution: The urgent need for cyber counterintelligence', *National Intelligence Journal*, vol. 1, no. 1, pp. 71-90.

Grant, MJ & Booth, A. 2009, 'A Typology of Reviews: An Analysis of 14 Review Types and Associated Methodologies', *Health Information & Libraries Journal*, vol. 26, pp. 91-108.

Heckman, KE, Stech FJ, Thomas RK, Schmoker B & Tsow AW 2015, *Cyber denial, deception and counter deception—A framework for supporting active cyber defense*, Springer International Publishing, Cham, CH.

Jaquire, VJ 2018, *A framework for a cyber counterintelligence maturity model*, Doctor of Commerce (Informatics) thesis, University of Johannesburg, South Africa.

Jaquire, VJ & von Solms, SH 2017a, 'Towards a cyber counterintelligence maturity model', *Proceedings of the 12th International Conference on Cyber Warfare and Security*, AR Bryant & RF Mills (eds), Wright State University, Air Force Institute of Technology, Dayton, OH, US, pp. 432-40.

——2017b, 'Developing a cyber counterintelligence maturity model for developing countries', *Proceedings of the 2017 IST–Africa Conference*, Windhoek, NA.

——2017c, 'Cultivating a cyber counterintelligence maturity model', M Scanlon & L Neihn-An (eds), *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, viewed 11 December 2018, <http://adam.uj.ac.za/csi/docs/ECCWS_2017_DSV_Prof_MS.pdf>, pp.109-19.

Justiniano, JE 2017, *Advancing the capacity of a theater special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone*, Master of Science (capstone project), Utica College, New York, NY, US.

Kim, JS 2018, *The importance of literature review in research writing*, viewed 10 January 2018, <https://owlcation.com /misc/literature_review>.

Knowles, JA 2013, *Applying computer network operations for offensive counterintelligence*, Master of Science (capstone project), Utica College, New York, NY, US.

Lee, RM 2014, 'Cyber counterintelligence: From theory to practice', *Tripwire (blog series 4)*, 4 May, viewed 4 January 2015, <http://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/>.

Mallett, R, Hagen-Zanker, J, Slater, R & Duvendack, M 2012, 'The benefits and challenges of using systematic reviews in international development research', *Journal of Development Effectiveness, v*ol. 4, no. 3, pp. 445-55.

Nakashima, E 2013, 'To thwart hackers, firms salting their servers with fake data', *Washington Post*, 2 January, viewed 22 July 2018, <https://www.washingtonpost.com/world/national-security/to-thwart-hackers-firms-salting-their-servers-with-fake-data/2013/01/02/3ce00712-4afa-11e2-9a42-1ce6d0ed278_story.html?noredirect=on&utm_term=.ab586f749056>.

Prunckun, H 2018, 'Weaponization of computers', *Cyber weaponry: Issues and implications of digital arms*, H Prunckun, (ed.), Springer, Cham, CH.

Putnam, RT 2015, *Digital mirrors casting cyber shadows—The confluence of cyber technology, psychology, and counterintelligence*, Master of Science (capstone project), Utica College, New York, NY, US.

Sigholm, J & Bang, M 2013, 'Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats', *Proceedings of the European Intelligence and Security Informatics Conference (EISIC), IEEE*, Uppsala, SE.

Stech FJ & Heckman KE 2018, 'Human nature and cyber weaponry: Use of denial and deception in Cyber Counterintelligence', *Cyber weaponry: Issues and implications of digital arms*, H Prunckun (ed.), Springer, Cham, CH.

Stone, GM & Bluitt, K 1993, 'Future law enforcement and internal security communications architecture employing advanced technologies', *IEEE Publication CH3372-0/93*, pp. 194 - 202.

Stone, GM & Tucker RS 1988, 'Counterintelligence and unified technical security programs', *Proceedings of the IEEE International Carnahan Conference on Security Technology: Crime Countermeasures*, New York, NY, US.

United States of America 2004, Department of Defense, *Dictionary of military and associated terms (12 April 2011 as amended through 7 October 2004)*, viewed 7 January 2018, <http://www.bits.de/NRANEU/others/jp-doctrine/jp1_ 02%2804%29.pdf>.

United States of America (U.S.) 2018, *Counterintelligence: Cyber threat*, Naval War College, viewed 2 August 2018, <https://usnwc.libguides.com/c.php?g=661096&p=4695517>.

University of Johannesburg 2018, *The Cyber Counterintelligence Project—Centre for Cybersecurity*, viewed 16 April 2018, <http://adam.uj.ac.za/csi/ CyberCounterintelligence.html>.

von Solms, SH 2014, 'Cyber counter-intelligence makes a difference', *ITWeb*, viewed 11 November 2014, <http://www.itweb.co.za/index.php?option=com_content>.

ANNEXURE I

Proceedings of the
17th European Conference on Cyber Warfare and Security
University of Oslo
Norway
28-29 June 2018

Edited by
Dr Audun Jøsang

A conference managed by ACPI, UK

acpi

Proceedings of the

17th European Conference on Cyber Warfare and Security ECCWS 2018

Hosted by
University of Oslo
Norway

28-29 June 2018

Edited by
Dr Audun Jøsang
University of Oslo, Norway

Review Process
Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy
ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:
http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academic-conferences-and-publishing-international-limited/

Conference Proceedings
The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

The Electronic version of the Conference Proceedings is available to download from DROPBOX http://tinyurl.com/ECCWS2018 Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.
The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-911218-86-9
E-Book ISSN: 2048-8610
Book version ISBN: 978-1-911218-85-2
Book Version ISSN: 2048-8602

Published by Academic Conferences and Publishing International Limited
Reading
UK
Tel: +44-118-972-4148
www.academic-conferences.org

Preface

These proceedings represent the work of researchers participating in the 17th European Conference on Cyber Warfare and Security (ECCWS) which is being hosted this year by University of Oslo, Norway on 28 - 29 June 2018.

ECCWS is a recognised event on the international research conferences calendar and provides a valuable platform for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the areas of Cyber Warfare and Security. It provides an important opportunity for researchers and practitioners to come together to share their experiences of researching in this varied and expanding field.

The first day will be opened with a keynote presentation by Siri Bromander who is part of the Threat Intelligence and Incident Response team at mnemonic, Oslo, Norway, will be speaking on *"Cyber Threat Intelligence (CTI)"*. Dr Olav Lysne of the Simula Research Laboratory, will then speak on the second day about *"Digital Vulnerability and International Interdependency"*.

With an initial submission of 137 abstracts, after the double blind, peer-review process there are 60 Academic Research papers, 10 PhD Research, 2 Masters Research, 2 Non-Academic and 1 Work in Progress paper published in these Conference Proceedings. These papers represent truly global research in the field, with contributions from Australia, Austria, Belgium, Finland, Germany, Greece, India, Ireland, Italy, Korea, Latvia, Lithuania, Malaysia, Netherlands, Norway, Portugal, Russia, South Africa, Sweden, Taiwan, USA, and UK.

We wish you a most interesting conference.

Dr Audun Jøsang
ECCWS Conference Chair
University of Oslo
Norway

Building the Ideal Cyber Counterintelligence Dream Team

Victor Jaquire, Petrus Duvenage, and Sebastian von Solms

Centre for Cyber Security, Academy of Computer Science and Software Engineering, University of Johannesburg

duvenage@live.co.za
jaquire@gmail.com
basievs@uj.ac.za

Abstract: "Years ago, small groups working together 'or lone wolves (ninjas)' were the ones who hacked into systems. The days of old have come and gone, and the criminals are now working together without fear of impunity more than ever" [Bodmer *et al*, 2012]. Bodmer *et al* [2012] also indicate that this situation is true for both the hacker and the defender, "as it is easier and safer to work in numbers on the Internet, especially since evidence collection and attribution are so difficult for all involved parties".

In a real world scenario where appropriate cyber counterintelligence (CCI) human resources are scarce and/or expensive and where limited relevant educational sources are available, it is imperative to identify the necessary people, teams and skills to anthropomorphise and mature the CCI effort in order to achieve an organisation's strategic CCI objectives.

In a world where suitable cyber related human resources are scarce and expensive, the process of identifying and building an appropriate, cost effective and functional CCI dream team is essential to ensure that an organisation's' CCI strategic initiatives are achieved.

This paper contributes to the series of previous papers on cyber counterintelligence (CCI) maturity. It aims to add to the emerging considerations on CCI through a discussion on a process of building an ideal CCI dream team as part of an organisation's CCI maturity. It highlights the effectiveness of cybersecurity when incorporating it in an integrated CCI approach. It further deliberates an integrative approach of CCI practices in conjunction with traditional defensive and/or offensive cyber measures in order to leverage on, and further develop existing skilled people. Lastly, it culminates in the discussion of the high level functions required within a CCI environment, setting the basis for putting together the ideal dream team as part of the establishment and / or maturity of a CCI capability that can be tailored for a government and/or private sector environment alike.

Keywords: cyber counterintelligence, dream team, cyber threat intelligence, defensive and offensive cybersecurity, cyber counterintelligence maturity

1. Introduction

Farchi [2016] refers to the requirement for counterintelligence within the private sector. He focusses on the need for a particular form of counterintelligence namely CCI and states that it entails utilising, '**defensive**' and '**offensive**' Counterintelligence **approaches**, with the aim of safeguarding organizations [Farchi, 2016]. In a conceptual overview and theoretical proposition Duvenage, von Solms & Corregedor [2015], describe CCI as "the subset of multi-disciplinary CI aimed at detecting, deterring, preventing, degrading, exploiting and neutralisation of adversarial attempts to collect, alter or in any other way breach the C-I-A (confidentiality, integrity and availability) of valued information assets through cyber means".

Farchi [2016] further refers to the escalating tendency of information security companies, emphasising their service offering on "gathering information on specific threats against organizations", instead of only the traditional focus on providing defensive solutions.

There are countless volumes written on various Intelligence, Counterintelligence and CCI concepts and approaches. Although some of the previous writings in this regard establishes the basis for CCI and focuses on some of these concepts, there is a notable lack in the availability of literature that provides guidance in both the form of a framework for a CCI maturity model, as well as the associated resources and skills required for such an undertaking.

The implementation of a CCI capability is dependent on an organisation's strategy, risk profile and unique requirements. The question then with regard to the requirements for relevant CCI people, skills or focus teams remains, since its requirements can be as diverse as the diversity of every organisation out there.

Due to the complexity of CCI, some guidance on identifying relevant people, skills, focus teams etc. is prudent that can assist organisations in transitioning their traditional defensive-only approach when securing cyberspace, to a more evolved approach in line with the demands for advanced threat mitigation of the present, and beyond. A beneficial starting point for such guidance (among others), emanates in the form of a discussion on an approach.

2. The Approach

A country, government and/or private sector business requires an efficient method to incorporate CCI within their whole security plan and to mature it over a set period into a fully functional CCI ability. This will include the implementation and maturity of CCI teams, skills and focus areas.

CCI is not necessarily a separate structure. It is rather a manner for existing and some new functionalities within the organisation to work together in a multi-disciplinary approach to achieve the CCI strategic vision and desired outcomes [Jaquire & von Solms, 2017 (1)]. In order then for an organisation to construct the ideal CCI team, it will be judicious to consider the functions that the CCI environment will perform within that organisation, in line with organisational strategy. This will allow the organisation to identify the CCI team functions accordingly, from which the ideal CCI team can be constructed. This will also provide the organisation with the opportunity to leverage on its existing resources, to assist in the implementation of the CCI capability in a cost effective way.

Even though there are CCI focus areas that will be identified in line with the organisational strategy for each different organisation, which will be specific to that organisation [Bardin, 2011], some base level functions, or grouping of functions will be the same within all organisations. These base level functions will form the foundation for the construction of any CCI team. From this core, further lower level functions and team requirements can be identified and implemented accordingly as per the organisations' needs and CCI maturity plan.

3. Constructing the ideal CCI dream team

When considering a CCI capability, all functions within a CCI maturity model can be grouped within five main high level functions [Jaquire, 2018]. These are the main functions that would be essential within all organisations, which require establishment and / or maturity for the purposes of a CCI capability. These main functions will form the centre for the constructing or identifying of an ideal CCI dream team and they are as follows:

1. **Senior Executive – C Level**
2. **Management**
3. **Analyses**
4. **Technical Specialisation**
5. **Incident / Situation Management and Coordination**

All five of these functions are principal to the effective functioning and maturity of all the Categories within CCI. From these five base functions, all further CCI sub-functions, resources and team requirement can flow in line with the organisational strategy. We will briefly discuss each of these functions within the following sections (Sections 3.1 to 3.5), relating each of them to the effort of building the ideal CCI dream team.

3.1. Function 1 - The Senior Executive (C-Level)

Kajava *et al* (2006) refer to the numerous information security awareness programmes within organisations, and stresses "top management often shies away from them". It is argued that the "damage caused by an individual employee may have far-reaching consequences for a company, but when damage is inflicted by senior management, the effects may be devastating" [Kajava *et al*, 2006].

Likewise, it is therefore not only imperative to ensure that the senior executive management endorse the CCI strategy, programme and efforts unequivocally, but also for the senior executive to understand CCI, cyber and

information security in order to take full control and responsibility thereof and actively participate and show their support [Kajava *et al*, 2006].

The senior executive is responsible for the overall strategy and direction of the organisation. CCI, just as is the situation with other organisational efforts, should be in line with the business objectives of the organisation. It is the senior executive who will decide the level of the intensity of focus on each of the dimensions within a CCI framework, as well as the level of maturity required for each of the dimensions within a CCI maturity model.

These decisions will be made in line with the strategic requirement of the organisation as per the organisations unique business realities, requirements and risk profile. These decisions include, among other, issues such as strategy development and approval (including CCI policy development and implementation), Financial Commitment and Strategic Operational Approval.

In order for the senior executive to make effective decisions, it is their responsibility to understand the cyber threats that the organisation faces, to understand the impact that a cyber-attack (in its various forms) can have on the assets of the organisation, and to instil this understanding and situational appreciation within the management and employees of the organisation.

For the senior executive to achieve this, they need to be skilled and trained to understand cyber-related threats that their organisation faces in line with their industry, area of business and own realities. They also need to be skilled and trained in appropriate remedial and proactive actions, as well as related strategies and thought processes in order to develop appropriate strategies and make informed decisions with regard to CCI for their organisation (*cf.* Duvenage, Sithole & von Solms, 2017). Senior executives should also be trained and skilled to fully understand CCI and the related CCI maturity model for their organisation, and they should ensure that the management below them are fully trained in this as well.

The senior executive function (accountable for the CCI programme) will therefore be the first essential part of the ideal CCI dream team.

3.2. Function 2 - Management

Management usually deals with general management issues such as (but not limited to) the following:

- Alignment with organisational strategy,
- Financial management,
- Operational management,
- Coordination,
- Approvals.
-

Within a technical, Information security or cyber related environment, managers also deal with the non-technical aspects of cyber and information security related issues such as the following [Soomro *et al*, 2016]:

- "Security policy development,
- Awareness and related training,
- Acquisition of security hardware and software,
- Internal control and decisions regarding data processing".

Due to the nature of such technical environments, there are numerous writings advocating the notion that "the safeguarding of information assets and data security can be ensured through the integration of technical and managerial activities" [Young & Windsor, 2010]. This is specifically the situation with regard to managers who are responsible for every condition within a multi-disciplinary CCI environment. Management, just as is the case with senior executives should be:

- Skilled and trained to fully understand the CCI environment under their control,
- Skilled and trained to fully understand:
    - How their environment fits into the larger CCI programme and strategy
    - What is required from their environment in line with the CCI effort

    - All the technical and non-technical processes and tasks to be performed by the technical and non-technical personnel and systems under their control – without necessarily becoming an expert on every field within their area of responsibility.
- Skilled and trained on the entire CCI process, especially the CCI maturity strategy and plan.

Apart from this, management should also, (in line with the training and skills development for senior executives), be trained and skilled in, among other:

- Threat identification, evaluation and management, including appropriate remedial and proactive actions,
- CCI methodologies including active, passive, defensive and offensive strategies, denial and deception techniques, operations and technical requirements.

Management should also realise their managerial authority and capabilities, especially when dealing with offensive and deception strategies, and be able to guide technical and non-technical personnel within their environment, in line with the organisational CCI strategy.

The CCI management function (responsible for the CCI programme) will therefore be the second essential addition to the ideal CCI dream team.

3.3. Function 3 - Analysis

In his benchmark contribution on Counterintelligence, Godson (2001) states: "Perhaps the queen of the counterintelligence chess board is counterintelligence analysis, both offensive and defensive." Since CCI is a subset of Counterintelligence, Godson's (2001) statement also rings true within CCI. This section argues the CCI analysis function as being:

- Multi-layered in that it pertains to appraisals on the tactical-technical, operational and strategic levels.
- Multi-disciplinary in that it draws from numerous fields of study, specialisation and expertise.
- An all-source endeavour in that it draws from data and information which could range from data feeds to information obtained from human sources. CCI thus includes, but is much wider than, data science.
- An appraisal process which combines various types of analysis – from automated technical analytics to analysis performed by humans.

Maisey [2014] reflects on the current automation of SIEM tools that "focus on automated, predictive analysis of attacks using data mining techniques as a way to reduce the load on analysts". He notes that the "idea is superficially attractive, and can be effective at spotting and preventing simple cases" [Maisey, 2014].

He further cautions that in situations like "fraud detection, similar tools have been found wanting against advanced adversaries such as organised criminals". He relates to the writings by Wilhelm [2014], who noted, "These adversaries are adaptive, and will change behaviour in order to evade specific detection tactics. Automatically derived rules tend to perform poorly when compared to those used by human analysts because they tend to focus on more robust indicators of fraudulent behaviour" [Willhelm, 2014]. Analysis (as one of the main drivers within the CCI domain), needs to heed these cautions [Maisey, 2014].

Analysis has both an internally and externally focussed responsibility. It is also the main player in identifying the level of CCI required within an organisation, based on the organisations strategic needs and unique environment. Borum *et al* (2014), allude to this type of analyses when referring to "Cyber-related considerations that matter in a strategic sense are the ones that impact an organization's ability to achieve its overarching mission objectives. Examples might include answers to the following [Borum *et al*, 2014]:

- "Does the organization operate in a high, moderate or low cybersecurity risk industry?
- What is the value of the organization's information and information flows to potential threat actors?
- What are the confidentiality, availability and integrity risks to the organization's assets?
- What legal liabilities exist related to the type of information stored, such as personally identifiable information…?"

Analysis further includes numerous fields of study, specialisation and expertise [Recorded Future, 2015], again depending on an organisations risk profile, strategic needs and unique environment, including, but not limited to analysis with regard to:

- Technical and non-technical defensive and offensive behaviours and strategies,
- Denial, deception and counter deception behaviours and strategies,
- Technical and non-technical behavioural and anomaly identification,
- Historical analyses,
- Predictive analyses,
- Predictive analytics – which can further be grouped under a region, a group of people, a country of origin etc.
- Trending – (Local, Regional, International),
- Language,
- Religion,
- Legal,
- Psychological and behavioural scientists,
- Data Science,
- HUMINT

The training and skills development requirement for CCI analysis needs to keep all these factors in mind to ensure that all requirements are efficiently addressed during the CCI maturity life cycle, in line with a Cyber Counterintelligence Maturity Model (CCIMM).

The analysis function will therefore be the third essential addition to the ideal CCI dream team. The specific analysis needs for each organisation will depend on the strategic CCI requirements of the organisation, and will include a focus on several of the areas within the analysis fields as listed above.

3.4. Function - Technical Specialisation

Seeing that CCI primarily focusses on counterintelligence within the cyber domain, technical operations (together with the analysis function as discussed above) forms the heart of CCI. Due to the numerous possible fields of technical focus within the cyber environment, technical specialisation in a multi-disciplinary approach (see the discussion within Sections 2 and 3.3), especially on a technical/tactical as well as an operational CCI level is essential.

To further strengthen this approach, in our experience the inclination is always there to split defensive and offensive operational and technical/tactical functioning. From a training and skills development point of view, there are major overlaps in the requisite training and skills requirements within both defensive and offensive requirements, as can be highlighted with the following figure:

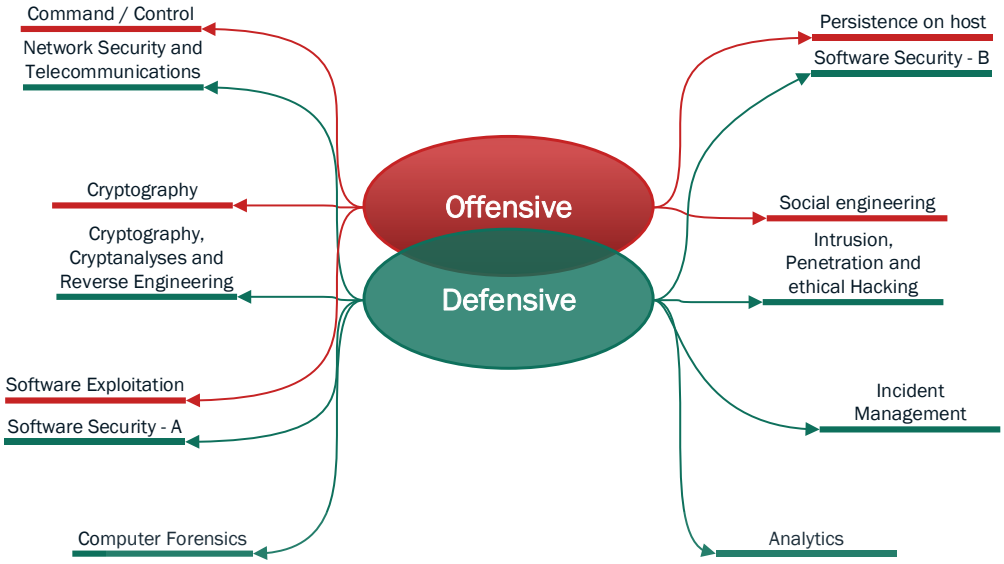


FIGURE 1: (NON-COMPREHENSIVE EXAMPLE) OVERLAP IN DEFENSIVE, OFFENSIVE CCI TRAINING, AND SKILLS DEVELOPMENT REQUIREMENTS (CREATED BY THE AUTHORS)

Even though Figure 1 is merely an example / extract and not an extensive comparison, and although there are specific areas of specialisation that are unique to each discipline (defensive or offensive) a definite functional skills overlap is noted within the requirements between Defensive and Offensive CCI. This at least as far as base knowledge is concerned, allowing for field of interest specialisation.

This integrative approach of CCI practices in conjunction with traditional defensive and/or offensive cyber measures can be done within both a government and/or private sector environment in order to leverage on, and develop existing skilled cyber and information security functions within a CCI environment.

It further indicates that the leveraging on existing cyber and information security functions within an organisation, allows for the cross functional utilisation of these same existing functions for the establishment and maturity of CCI in a CCIMM.

It also further strengthens the notion that cyber counterintelligence is not necessarily a separate unit within an organisation. As indicated earlier, CCI is therefore, more often than not, not a structure, but rather a way of 'functioning', through the maturity of existing and new functionality within an organisation to fulfil the CCI requirement - to achieve the CCI strategic vision and desired outcomes in a cost effective manner.

To this end, structures and activities that we might acknowledge as forming part of the cyber and information security realm can be allocated to each of the five CCI dimensions [Jaquire & von Solms 2017(2)].

Although this may vary from organisation to organisation, the allocation can be demonstrated within an example look as follows (see Figure 2):

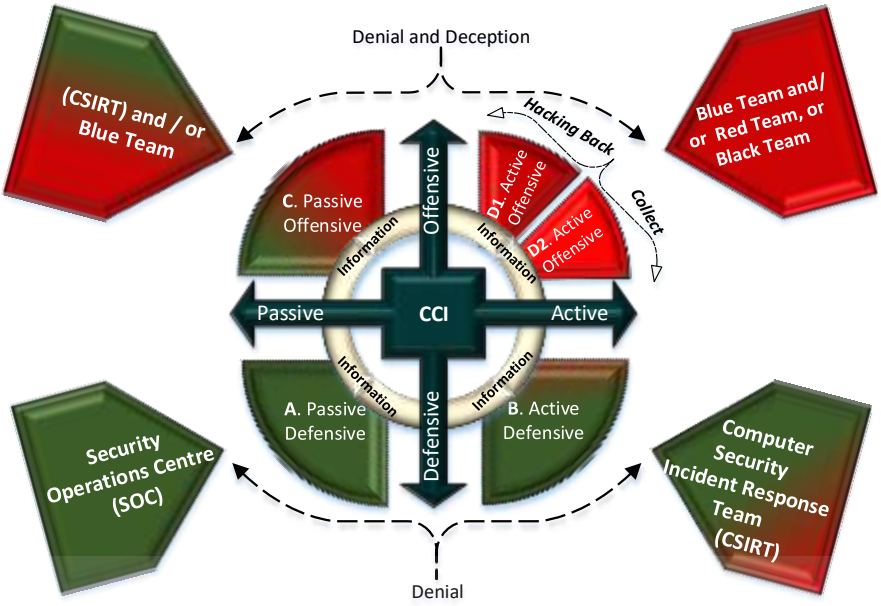


FIGURE 2: EXAMPLE OF AN ALLOCATION OF EXISTING FUNCTIONS / ACTIVITIES PER CCI DIMENSION (CREATED BY THE AUTHORS)

When studying Figure 2, we can utilise a basic Computer Security Incident Response Team (CSIRT) structure as an example (this structuring will be uniquely customised by each different organisation). In this example, the CSIRT is the main entity responsible for the activities allocated to the **Active Defensive** dimension (B), as well as a contributing entity responsible for the activities within the **Passive Offensive** dimension (C).

In an organisation, the CSIRT, for example, might be an existing functioning structure with existing specified activities to fulfil in line with the organisational strategy. In order to integrate this structure into the integrated CCI effort, its existing activities can be taken into account in order to slot them in correctly with the organisations own customised **CCIMM**, within the correct dimension. Examples (non-exhaustive) of CSIRT activities within the **Active Defensive** dimension may for instance include the following:

- *Alerts and warnings*
- *Vulnerability assessments and penetration testing*
- *Secure code analyses*
- *Artefact handling*

Further examples (non-exhaustive) of CSIRT activities within the **Passive Offensive** dimension may, among other, include the following:

- *Implementation, monitoring and analysis of honeynets,*
- *Implementation, monitoring and analysis of tar pits and sandboxing,*
- *Identification and location tracking of perceived threatening IP addresses.*

In examples like these, the exiting activities of the CSIRT within the organisation will form part of the organisations own customised **CCIMM** and will, because they are already existing activities, already be on a higher stage of maturity than the activities that are specified within a **CCIMM**, but which are not currently performed by such a CSIRT. All of these existing and newly identified activities need can then be specified within the organisations **CCIMM** within the sub-categories as Compliance Indicators. In the same way, all other relevant existing functions within the organisation can be integrated within the CCI programme to ensure that existing technical expertise, specialisation and technical generalists are utilised.

The technical specialisation function will therefore be the fourth essential addition to the ideal CCI dream team. As is the case with the analysis function, the specific technical specialisation skills or team focus requirements (examples of which are highlighted within domains A to D within Figure 2), as well as its intensity of utilisation will depend on the organisations CCI strategy.

3.5. Function 5 - Incident / Situation Management and Coordination

Kulikova et al [2012], indicate that "security incidents vary widely in their severity", and that "the composition of the incident response team should reflect the impact the incident has on the organization" [Kulikova et al, 2012]. In the same way, throughout the CCI process, all CCI related outcomes, situations, incidents and efforts needs to be coordinated and managed accordingly.

Although the day-to-day management of the CCI environment is done by the relevant management, and although basic incidents are handled through the normal cyber incident-management functions, certain events and/or situations require a dedicated control from the moment that it is conceived or identified, until fruition and post mortem evaluation.

Either these situations can be planned activities flowing from strategic, operational or technical/tactical needs, or they may originate as a result of the analyses outcome, based on the various analyses spheres [as discussed within Section 3.3 above], such as specific incidents reported from the operational or technical/tactical environment.

This function can also be described as a specialised project management function, which requires extensive insight within the CCI field, as well as extensive experience with regard to CCI, the CCI maturity life cycle and within the different CCI related domains. It especially requires extensive knowledge and experience within the CCI analysis field as in our experience, continuous situational analyses throughout the process is required.

As an example. The incident / situation management and coordination function includes, among other, the following:

- Coordination of Incident / situation handling efforts between strategic, operational and technical / tactical environments, including:
    - Escalation.
    - Resolution authorisation (when the resolution of a specific situation requires approval from management or the executive),
    - Incident / situation handover – Should the handling of the incident or situation require expertise and / or resolution by a third party or external organisation.
- Inter programme coordination of incident / situation handling efforts and resolution,
- Inter organisational coordination of incident / situation handling efforts and resolution

The incident / situation management function will therefore be the fifth and last essential addition to the ideal CCI dream team.

4. Conclusion

In today's reality, the defensive-only solutions, habitually trusted throughout the decades are no longer sufficient to safeguard our environments and our way of life. The advancement of solutions to recognise and deal with the assaults against the confidentiality, integrity and availability of information and infrastructure endures as decisive defensive measures, but it is no longer efficient as a comprehensive resolve.

As identified within the approach, an organisation requires an efficient method to incorporate cyber counterintelligence within their whole security plan and to mature it over a set period into a fully functional cyber counterintelligence ability. This approach will include the implementation and maturity of CCI teams, skills and focus areas.

Constructing a CCI team is very much dependent on what the organisation aims to achieve within its CCI strategy. Building the ideal CCI dream team will require careful consideration between current functions, new functions and costs.

Following a multi-disciplinary and integrated methodology can assist an organisation to utilise its existing skills, teams and functions, together with newly identified requirements as highlighted within its CCI maturity strategy, in order to realise these strategic team requirements.

The approach to align team considerations with the five main functions that would be essential within all organisations for the establishment and / or maturity of a CCI capability, is a promising starting point in building the CCI team. This team can further evolve, together with all the other focus areas as highlighted within an organisations CCI maturity strategy, towards the ideal cyber counterintelligence dream team.

References

Bardin, J. (2011), 'Ten Commandments of Cyber Counterintelligence' - Adapted from James M. Olson , *CSO online*, http://www.csoonline.com /article /2136458/ identity-management / ten-commandments –of - cyber- counterintelligence ---adapted –from –james –m –olson .html, Accessed 18 Feb 2016

Bodmer, S. *et al* (2012), *Reverse deception–Organized cyber threat counter- exploitation*, McGraw-Hill, New York.

Borum, et al (2014), 'Strategic Cyber Intelligence', *Emerald Insight, Information and Computer Security*, Vol 23, No 3, pp 317-332, www.emeraldinsight.com/2056-4961.htm, Page 322.

Duvenage, von Solms, & Corregedor (2015), 'The Cyber Counterintelligence Process - a conceptual overview and theoretical proposition', Paper read at the *14th European Conference on Cyber Warfare and Security, (ECCWS)*, Hatfield, United Kingdom, July 2015.

Duvenage, P.C., Sithole, T.G. & von Solms, S.H. (2017) 'A conceptual framework for cyber counterintelligence – Theory that really matters!' in *Published Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland,

June.Godson, R. (2001) *Dirty tricks or trump cards – U.S. covert action and counterintelligence*, Transaction Publishers, New Brunswick..Heckman, et al (2012), *Cyber Denial, Deception and Counter Deception, A Framework for Supporting Active Cyber Defence*, Springer.

Jaquire, V.J. (2018), *A framework for a cyber counterintelligence maturity model*, unpublished Doctor of Commerce (Informatics) thesis at the University of Johannesburg, Johannesburg, South Africa, Chapter 8.

Jaquire, V. & von Solms, S.H. (2017(1)), 'Cultivating a Cyber Counterintelligence Maturity Model', paper read at the *16th European Conference on Cyber Warfare and Security*, (ECCWS).

Jaquire V. & von Solms S.H. (2017(2)), Towards a Cyber Counterintelligence Maturity Model, *ICCWS 2017*.

Kajava, et al (2006), *Senior Executives Commitment to Information Security - from Motivation to Responsibility'*, University of Lapland, IEEE 1-4244-0605-6/06, Accessed 20 Feb 2017

Kulikova, et al (2012), 'Cyber Crisis Management: A decision-support framework for disclosing security incident information, *2012 International Conference on Cyber Security*, Page 106.

Maisey, M. (2014), Moving to analysis-led cyber-security, Science Direct, http:// www.sciencedirect.com /science /article /pii/S1353485814700492, Page 7, Accessed 10 March 2017

Recorded Future, (2015), *Temporal Analytics for Predictive Cyber Threat Intelligence*, https://www. recordedfuture.com/category/product/ , Page 868

Soomro, et al (2016), Information security management needs more holistic approach: A literature review, *International Journal of Information Management*, 36 (2016) 215–225, Page 219

Willhelm, W.K. (2014), The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management, *Journal of Economic Crime Management*, Spring 2014, Volume 2, Issue 2,. https://library. utica. edu/ academic/ institutes/ ecii/ publications/ articles/ BA309CD2-01B6-DA6B- 5F1DD7850BF6EE22.pdf, Accessed March 2017

Young & Windsor, (2010). Empirical evaluation of information security planning and integration, *Communications of the Association for Information Systems*, 26(1), 245–266.

ANNEXURE J

ICCWS 2019

Stellenbosch, South Africa

14th International Conference on Cyber Warfare and Security

Stellenbosch University

28 February -1 March 2019

ISBN 978-1-911218-74-6

For further information contact
info@academic-conferences.org
or telephone
+44-(0)-118-972-4148

Eating the Elephant - A structural outline of Cyber Counterintelligence Awareness and Training

Thenjiwe Sithole, Petrus Duvenage, Victor Jaquire and Sebastian von Solms
Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa
duvenage@live.co.za
thenjiwes@icloud.com
jaquire@gmail.com
basievs@uj.ac.za

Abstract: It is widely acknowledged that conventional cyber security solutions alone are wholly insufficient in the face of threats posed by role players such as nation states, criminal syndicates, corporate spies, terrorists, hacktivists and rogue individuals. The securing of cyber space depends not only on raising the bar in respect of defensive measures, but also needs to involve proactive action focussing on threat agents. For organisations with sizable assets, cyber counterintelligence (CCI) offers a practicable approach which combines both the defensive and offensive dimensions. CCI's effective implementation and execution above all requires a coherent organisational awareness and training programme (ATP). For larger organisations, A cyber counterintelligence awareness and training programme (CCI ATP) programme has to be multi-tiered and will typically range from the elementary (e.g. basic cybersecurity awareness and skills training for all personnel) to the advanced (e.g. courses for CCI specialists on the cyber frontlines). The design of such a multi-tiered programme is self-evidently a daunting task and published academic research on this topic is very limited. This proverbial elephant thus needs to be eaten one bite at a time. This paper advances three such first 'bites', namely (i) the conceptualisation and contextualisation of a CCI ATP; (ii) a proposition on the structuring of the CCI ATP's design and implementation process; and (iii) a high-level structuring of a multi-tiered CCI ATP. The multi-tiered CCI ATP we advance in this paper consists of four tiers which are explicated with reference to *inter alia* target group, training objectives and training content. The paper concludes with observations on the CCI ATP research conducted thus far.

Keywords: Cyber security, cyber counterintelligence, offensive cybersecurity, threat intelligence, training.

1. Introduction

Cyber security is a continuously changing and fast growing field which demands of an organisation's work force at all levels to keep up the pace. It is also widely acknowledged that conventional cyber security solutions alone are wholly insufficient to deal with sophisticated and fast-growing cyber risks and threat actors who take advantage of vulnerabilities availed by emerging technologies. There is growing recognition that the security and prosperity of organisations require a more proactive, intelligence-driven approach in mitigating cyber risks. Especially for larger organisations with sizable interests such a proactive approach need to incorporate cyber counterintelligence (CCI). CCI can be defined as measures to "identify, deter, exploit, neutralise and protect against adversarial attempts to collect, alter or in any other way breach the C-I-A [confidentiality, integrity and availability] of valued information assets and where cyber is a principal instrumentality and/or a target" (Duvenage & von Solms, 2013; Duvenage & von Solms, 2015).

CCI's effective implementation and execution above all requires a skilled CCI workforce as well as CCI-conscious employees. Such awareness and skilling is best achieved as part of an organisation's broader CCI awareness, education and training (AET) endeavour. Ideally, this CCI AET endeavour would have a multi-tiered CCI training and awareness programme (CCI ATP) as a main thrust. The design and implementation of a CCI ATP is a daunting task. Factors contributing to the complexity of this task include the following:

- Unclassified information and research on CCI ATP is scarce. This can in part be ascribed to CCI being a relatively new academic field with very limited published academic research on CCI awareness, education and training in general. In as far as surveyed literature is concerned, only two (outstanding and commendable contributions) could be found, namely (Black, 2014; Van Derwerken & Ubell, 2011)
- CCI cuts across multiple disciplines and involves several skillsets. Ideally, CCI ATP would draw an all these disciplines and skillsets – with self-evident implications for the (CCI ATP's) design process.

- Organisations differ vastly not only in strategic objectives, but also in their workforces' CCI-relevant skilling and awareness. Therefore, there is no 'one-size-fits-all' CCI ATP. Instead, a CCI ATP's design should be congruent with an organisation's unique features and strategic objectives.

As is clear from the above, the design of a CCI ATP is a proverbial elephant that needs to be eaten one bite at a time. This paper advances three such first 'bites', namely:

- Conceptualisation and contextualisation of a CCI ATP.
- A proposition on the structuring of the CCI ATP's design and implementation process.
- A high-level structuring of a multi-tiered CCI ATP.

In this section we motivated the need for CCI ATP and highlighted some challenges pertaining to the design of such a programme. Subsequently, we introduced the three propositions this paper aims to advance. In the next section, we discuss the first of these propositions, namely CCI ATP's conceptualisation and contextualisation.

2. Conceptualising and contextualising of a CCI ATP

Conceptually, and in practice, an effective CCI ATP is designed with due cognisance of an organisation's (i) strategy, intelligence and counterintelligence efforts and (ii) CCI broader awareness, education and training (AET) endeavour.

An effective CCI ATP is thus not a standalone 'plug in' or 'add on'. An effective CCI ATP is conceptualised and executed as part of the broader organisational CCI awareness, education and training (CCI AET) endeavour. The AET in turn forms part of the wider organisational strategy, intelligence and counterintelligence efforts. This interconnectedness, which will ultimately shape the CCI ATP's design, is graphically depicted in Figure 1:

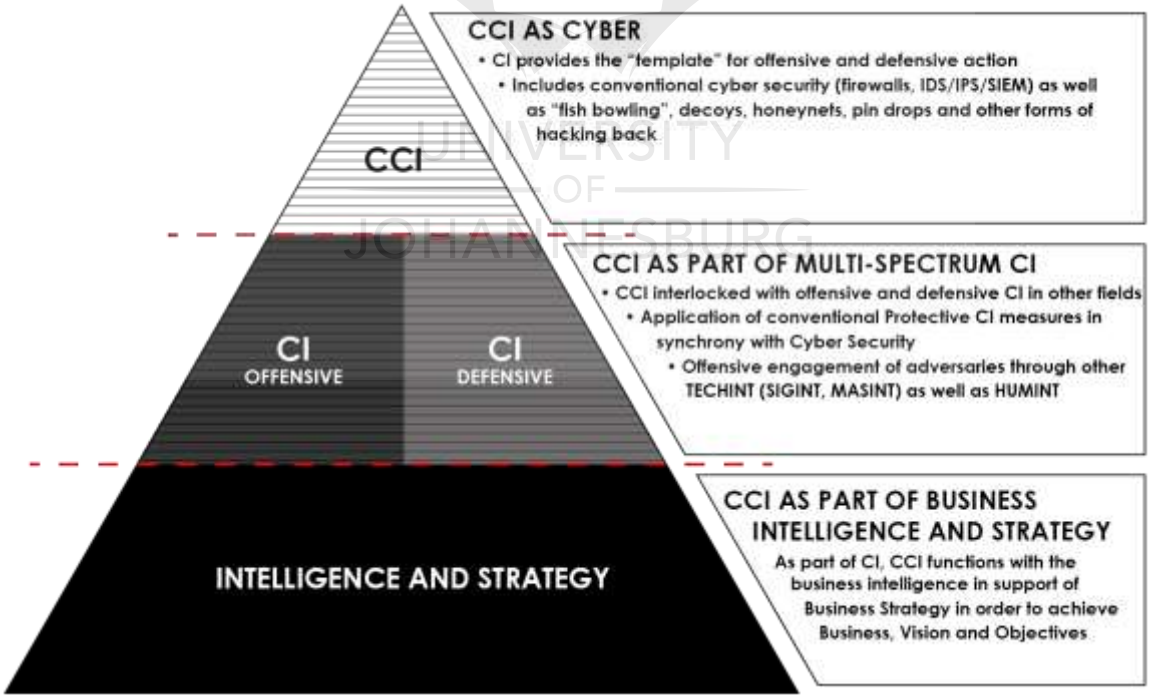


Figure 1: CCI three-tiered relationship with Strategy, CI and Cyber *(*Duvenage & von Solms, 2015*)*

The design, development and implementation of a CCI AET is typically dependent on objectives described in an organisation's holistic AET policy. CCI AET is further dependent on the expertise of workforce that the organisation already has and the target group, that is, does the organisation has an assigned CCI team? If not,

does the organisation need to train the existing counterintelligence (CI) personnel in cyber or existing cyber workforce in CI, or recruit new personnel to be trained in the CI and cyber? In this regard, care should be taken not to confuse CCI as being a duplicate to cyber security. Instead, CCI is a combination of traditional CI and cyber security as well as advanced technical abilities (Black, 2014). Figure 1 shows CCI as being proactive and including offensive dimensions. It is therefore linked with, but goes beyond cyber risk management.

A skilled specialised CCI team alone, however, is insufficient. In fact, most smaller organisations will not have such a dedicated team. In this regard, Jaquire, Duvenage & von Solms (2018) state:

> CCI is not necessarily a separate structure. It is rather a manner for existing and some new functionalities within the organisation to work together in a multi-disciplinary approach to achieve the CCI strategic vision and desired outcomes.

In addition, employees in general remain the weakest link in the organisational armour and continue to be the main reason of data breaches resulting from cyber incidents link (Thomason, 2013; Monk, *et al* 2010; Dtex, 2017). Since it is important that every employee know and understand their roles and responsibilities, a CCI AET has to, at the very least, provide for CCI awareness to all employees regardless of occupational group.

As AETs in general, a CCI AET should thus not be considered as a single, uniform "training" program but as having three different functions, namely 'Awareness', 'Education' and 'Training' (cf. Kissel & Wilson, 2010). Each of these functions differs in target group, specific objectives, outcomes, content and approaches (Kissel & Wilson, 2010). These functions can be differentiated in more detail as follow:

- **Awareness** is about being cognisant or knowledgeable of a situation or one's surrounding. It is an AET's critical base function - the first line of defence that affords employees with an opportunity to learn about the importance of personal security as well as protecting organisation's critical information systems assets. The NIST Special Publication 800-16 defines an awareness as "a learning process that sets the stage for training by changing individual and organisational attitudes to realise the importance of security and the adverse consequences of its failure" (de Zafra, *et al*., 1998).

- **Education** is about the facilitation of learning or teaching and the gaining of knowledge. Caballero (2017) defines education as "a formal curriculum created for the purpose of educating individuals in a broad array of security topics that will build a body of knowledge essential for a career in information security" (Caballero, 2017).

- **Training** is about the acquisition of competence (knowledge, skills and attitude) to improve performance and enhance expertise for a specific job or function. Amankwa *et al* (2014) define training as "any endeavour that is undertaken to ensure that every employee is equipped with the information security skills and information security knowledge specific to their roles and responsibilities by using practical instructional methods such as seminars and workshops" (Amankwa, Loock & Kritzinger, 2014)

For purpose of this paper, 'Education' is deemed as a function provided by tertiary and training institutions outside the organisation. Our proposition in this paper, however, centres on an *organisational* CCI awareness and training programme (ATP). The CCI ATP thus *excludes* 'Education' but *includes* 'Awareness' as its first proficiency level. Our CCI ATP then subdivides the 'Training' function in three further proficiency levels namely: fundamental, functional and advanced. These resultant four proficiency levels of our CCI ATP can graphically be depicted as follow:

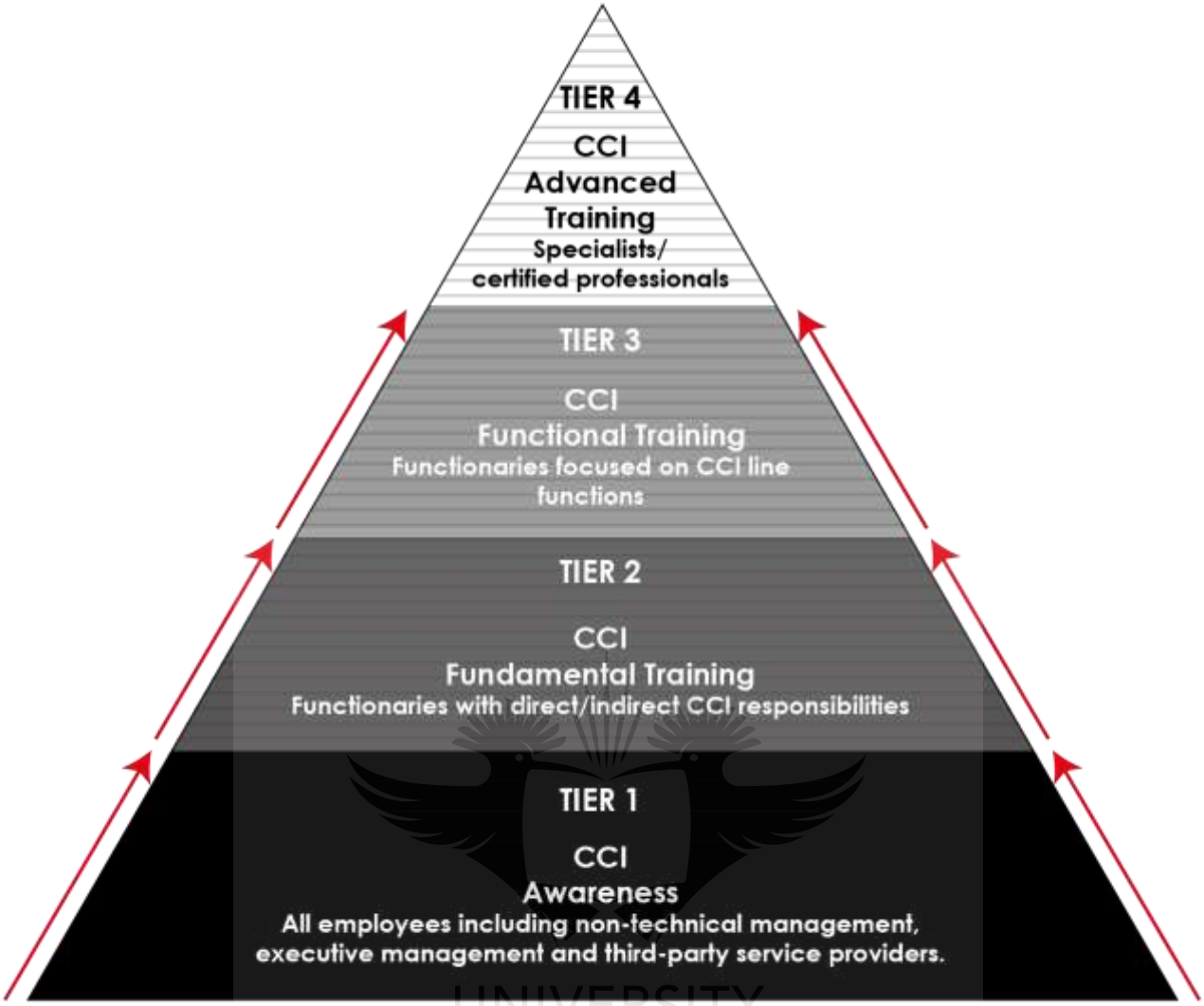


Figure 2*: Proficiency Levels (Tiers) of a Cyber Counterintelligence* Awareness *and* Training Programme *(CCI ATP) (Authors)*

This section conceptualised and contextualised a CCI ATP as part of organisational strategy and the organisation's broader awareness, education and training (AET) endeavour. This was done to infer the four proficiency levels of a CCI organisational awareness and training programme (CCI ATP). In the next section we advance a structural outline for the process by means of which the CCI ATP can be designed and implemented.

3. Structural Outline of the CCI ATP's Design and Implementation Process

The proficiency levels as discussed in the previous section, provide a scaffold for the design and implementation of a CCI ATP. This design and implementation are done by means of structured process comprising the four steps depicted in Figure 3:

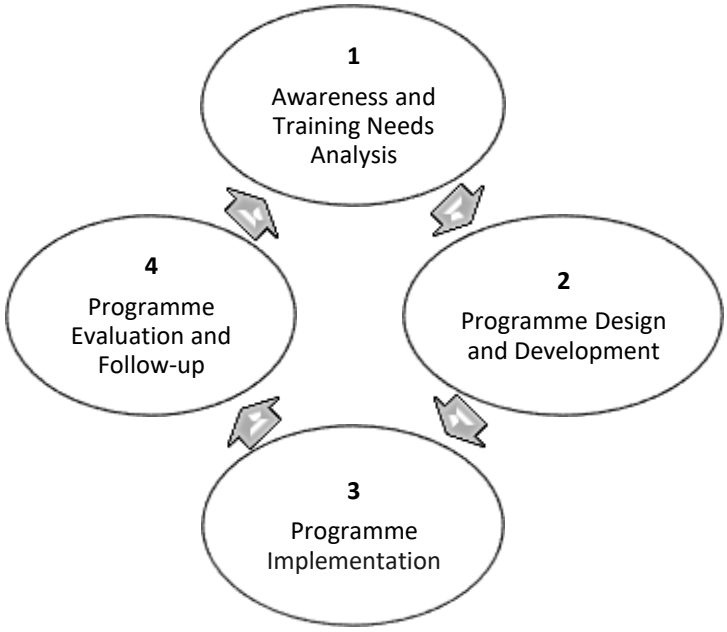


Figure 3: CCI ATP Design and Implementation Process (adapted from MacCauvlei Learning Academy, 2016)

The four critical steps, depicted in Figure 3, that need to be followed for the CCI ATP's design and implementation, can concisely be described as follow (adapted from MacCauvlei Learning Academy, 2016):

1) An **awareness and training needs analysis** determines the organisation's awareness and training needs according to the strategic objectives. It looks at the skills and knowledge required by the workforce generally and the CCI team specifically, with due cognisance of the organisation's strategy well as its intelligence and counterintelligence thrusts.

2) The **programme design and development** derives the programme objectives from the training needs and then design and develop the training material. It determines content, the duration of the programme, the training methods and techniques. The three proficiency of CCI training (fundamental, functional and advanced – see Figure 2) will be designed according to the functional specialities such as CCI collection, CCI analysis, CCI investigation, CCI offensive and CCI defensive

3) The **programme implementation,** communicates the training implementation to the respective target groups and their management echelons. Various training methods can be used for the implementation of awareness and training, such as classroom, online, practical, simulations, on-the-job training and so on.

4) **Programme evaluation and follow-up** appraises the effectiveness of the programme in terms of the increase in knowledge and skills and the improvement of attitude on the job as a result of the awareness and training programme. Follow-ups are done in the workplace after a certain period about the sustainability of knowledge, skills and attitude.

In this section, we advanced a structured process which can be applied for the design and implementation of a CCI ATP. In the next section a high-level outline of the programme itself is provided.

4. A High-level Outline of the multi-tiered CCI Awareness and Training Programme

A multi-tiered CCI Awareness and Training Programme (CCI ATP) can of course not be presented in any detail within the confines of a conference paper. In this section we thus only provide some high level contours of a CCI ATP. To this end, we discuss each of the four proficiency levels (see figure 2) with reference to the key elements of target group, objectives, content and delivery methods and techniques.

4.1 CCI Awareness – the first line of defence and offence (Tier 1 – Figure 2)

Since employees cannot protect information systems against something they are oblivious of, e CCI awareness is a foundation and fundamental to enlighten employees of the cyber threats faced individually and as an organisation. A CCI awareness programme is a first line of defence and a foundation for the stronger cyber security posture of an organisation. Awareness focuses on people rather than technology with the key purpose of an awareness programme is to direct the attention of people to information security (Toth & Klein, 2013) It conveys the possible cyber risks and cyber threats faced by the organisation and provides skills to mitigate basic cyber-related risks and counter cyber threats (Roper, Grau, & Fischer, 2006).

The key elements of CCI awareness are as follow:

1) Description: A blended cyber security and CI awareness programme that increases employee awareness on the cyber threat landscape, type of adversaries and their techniques, and provide appropriate countermeasures. The emphasis is on personal and workplace practices which will limit the risk of individuals being exploited as an attack vector.

2) Target group: All employees including new employees, contractors and, in some instances, third-party service providers.

3) Objectives**:** After completing the awareness, individuals will be able to
   - Identify basic cyber threats and risks,
   - employ sound personal and workplace cyber security practices,
   - be aware of critical organisational assets,
   - be aware of the exploitation of the human element as attack vector,
   - understand policies and procedures to secure information systems, and
   - understand and recognise the countermeasures.

4) Overview of content
   - Cyber risks, cyber threats and cyber attacks
   - what is CI and CCI
   - policies and procedures
   - insider threat
   - techniques used by cyber actors
   - data security and privacy
   - personal security
   - computer and mobile security
   - internet and email security

5) Delivery methods and techniques.
   Several methods or techniques can be used to deliver an awareness programme, namely classroom tuition, workshops, online courses, seminars and open lectures. Supplementary techniques include intranet postings, posters, videos, games, quizzes, screensavers, etc

4.2 CCI Fundamental Training (Tier 2 – Figure 2)

CCI training, to reiterate is essential for improving the effectiveness of the organisation in achieving its strategic objectives. Training addresses employee competencies (knowledge, skills and attitude), skills gaps, re-skilling and upskilling. Training programmes are structured according to proficiency levels (fundamental, functional and advanced – see figure 2) and customised, where relevant, as *per* the requirements of functions or roles.

Since CCI training is multi-disciplinary, fundamental training should transfer a sound grasp of CCI as subset of counterintelligence and intelligence. It should also convey the CCI modes of active-offensive, active-defensive, passive-offensive and passive-defensive. To this end, the eight notional building blocks described by Duvenage,

Sithole & von Solms 2017) in their' Framework for Cyber Counterintelligence' could be of value. This framework can graphically be depicted as follows:

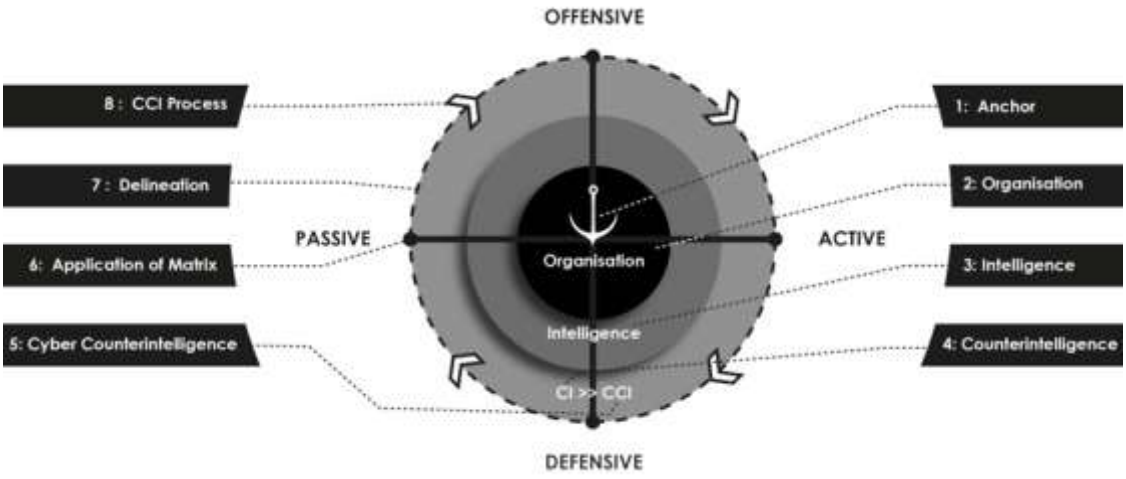


Figure 5: Conceptual Framework for Cyber Counterintelligence (Duvenage, Sithole, von Solms 2017)

CCI fundamental training is an entry level for functionaries with direct/indirect CCI responsibilities and serves as the foundation for functional and advanced training later on.

The key elements of CCI functional training can be summarised as follow:

1) Description: A blended cyber security and CI training that is a bridging programme between CCI awareness and CCI functional training. This level covers a fundamental understanding of CI skills, computer hardware, software, networks and systems. It introduces both offensive and defensive domains so that CCI team at the fundamental level will be able to, on a basic level, counter cyber intelligence threats

2) Target group: Functionaries with direct/indirect CCI responsibilities CI and personnel wanting to enter the CCI realm.

3) Objectives**:** After completing after completing fundamental training, individuals will
   - be equipped with knowledge, skills and tools to counter cyber threats,
   - understand the cyber threat landscape,
   - understand software security, networks security and systems security vulnerabilities,
   - understand and can apply software security, networks security and systems security measures,
   - have been introduced to basic offensive and defensive CI, cyber warfare and CCI strategies, and
   - be able to demonstrate CI and fundamental CCI skills.

4) Overview of content
   - Information Technology Security (computer security, networks security, data security)
   - Physical security
   - Cyber Threat landscape
   - Cyber actors and attack vectors
   - Cyber intelligence (cyber collection)
   - Social Media and its role to cyber collection, threats and attacks
   - Policies, Procedures and Standards (CI, Information and Cyber Security)
   - Fundamentals of aspects such as penetration testing, cryptography, digital forensics, etc.
   - Cyber resilience or cyber risk management based approach.

5) Delivery methods and techniques.
Several methods or techniques can be used to deliver a fundamental programme, namely classroom tuition, online, hands-on or virtual and practical.

4.3 CCI Functional Training (Tier 3 – Figure 2)

CCI functional training is at an intermediate level. It is a role-based training because it is structured according to the roles and responsibilities of the CCI job or position, depending on how the CCI function is structured in an. Design and development of the training curriculum will differ according to specific skills as required by a particular role. Some of the suggested roles such as CCI investigation, CCI Analysis, CCI Collection organisation, CCI technical specialisation (Black, 2014; Jaquire, et al., 2018).

1) Description: A blended cyber security and CI training that builds on the knowledge and skills acquired in the fundamental CCI training. This training structured according to the roles and responsibilities of the CCI job or position.

2) Target group: The training for CCI workforce and all functions in both CCI offensive and defensive domains.

3) Objectives: After completing the awareness, individuals will be able to

- equipped with knowledge, skills, attitude and tools to conduct CCI functions according to specific domain.
- As CCI is multi-disciplinary, some of the training objectives and skills development will overlap as illustrated by Jaquire, et al. (2018) in figure 5.

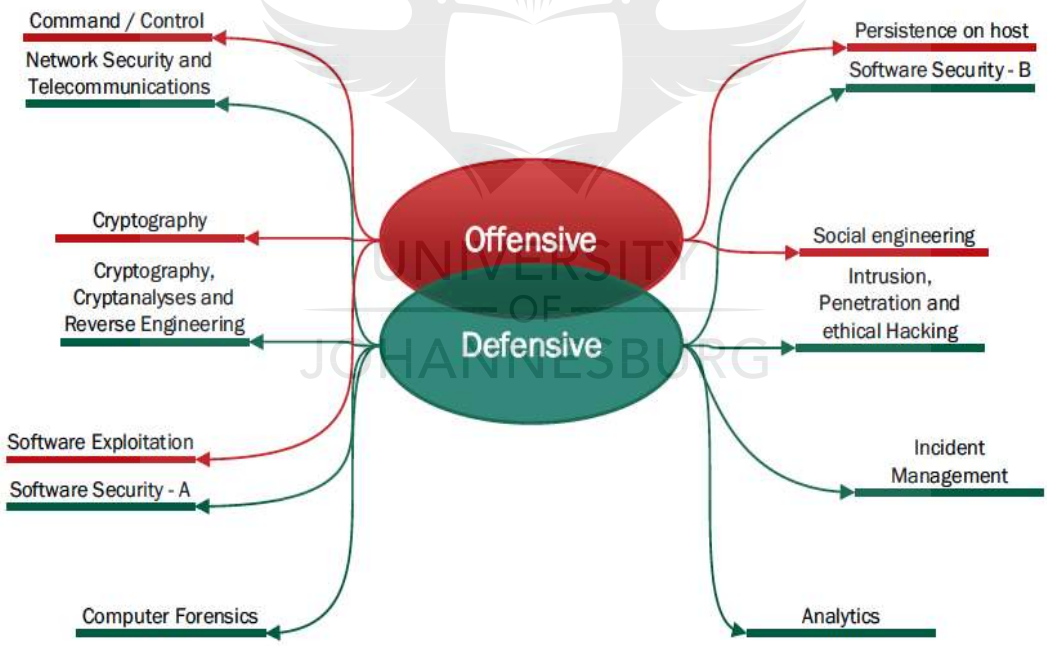


Figure 5: (Non-comprehensive example) overlap in defensive, offensive CCI training, and skills development - (Jaquire, Duvenage, & von Solms, 2018).

4) Overview of content - the topics are for both offensive and defensive CCI training, the list is not exhaustive. Each topic can be broken down into sub-topics.

- Cyber threat intelligence
- Data collection: OSINT, HUMINT & SOCMINT
- Digital Forensics
- Advanced networks
- Cryptography

- Penetration testing
- Vulnerability assessment
- Exploitation
- Ethical hacking
- Incident response management
- cyber intelligence analysis
- data analytics

5) Delivery methods and techniques

There are many methods or techniques that exist to deliver a functional training programme: classroom, online, hands-on or virtual practical, cyber games, emulation and simulation exercises (blue team, red team), research.

4.4 CCI Advanced Training (Tier 4 – Figure 2)

This training proficiency level equips individuals with relevant specialist knowledge and skills. According to Toth & Klein (2013), this level "integrates training, education and experience with an assessment mechanism to validate knowledge and skills, resulting in the 'certification 'of a predefined level of competence". For a certain part, this level of training thus draws on industry-based knowledge. Serving as examples are the training and assessment conducted by external certification bodies such as EC-Council, ISACA, (ISC)², SANS and CompTIA. Within statutory state security structures internationally, however, external industry-based training is complemented by advanced in-house training in especially CCI's offensive dimensions.

5. Conclusion

Cyber counterintelligence offers a proactive approach in countering cyber threats and cyber-attacks. This paper presented the outlines of a four-tiered CCI training programme with reference to *inter alia* target group, training objectives, training content and delivery methods or techniques. The design and development of the CCI ATP must follow the four step training cycle as it will ensure continuous update and relevance of the content.

The CCI ATP's proficiency levels discussed were awareness, fundamental training, functional training and advanced training. All these levels have content that incorporates both the CI and cyber skill sets. Within the confines of a conference paper only some contours of CCI ATP could be provided. Furthermore, and for self-evident reasons of sensitivity, some aspects of functional and advanced CCI training are not reflected in academic research in the public domain.

References

Amankwa, E., Loock, M., & Kritzinger, E. (2014). 'A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions', *The 9th International Conference for Internet Technology and Secured Transactions* (ICITST-2014) (pp. 248-252). IEEE.

Black, J. M. (2014). *The Complexity of Cyber Counterintelligence Training*, Master of Science in Cybersecurity, Utica College. Unpublished.

Caballero, A. (2017). 'Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems' in J. R. Vacca (dd.), *Computer and Information Security Handbook* (Third Edition) (pp. 393-419). Morgan Kaufmann.

Caballero, A. (2017). 'Security Education, Training, and Awareness' in *Computer and Information Security Handbook* (Third Edition) (pp. 497-505). Morgan Kaufmann.

de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998, April). NIST, National Institute of Standards and Technology. Computer Information Resource Center. Information Technology Security Training Requirements: a Role- and Performance-Based Model. Retrieved September 2018, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

Dtex. (2017). *2017 Insider Threat Intelligence Report*. Retrieved October 2017, from Dtex Systems: https://www.dtexsystems.com/2017-insider-threat-intelligence-report/

Duvenage, P., & von Solms, S. (2013). 'The Case for Cyber Counterintelligence', *International Conference on Adaptive Science and Technology*. Pretoria, South Africa: IEEE.

Duvenage, P., & von Solms, S. (2015). 'Cyber Counterintelligence: Back to the Future', *Journal of Information Warfare*, 13(4), 42-56.

Duvenage, P., Sithole, T., & von Solms, S. (2017). 'A Conceptual Framework for Cyber Counterintelligence – Theory That Really Matters', 16th *European Conference on Cyber Warfare and Security*, (pp. 109-119). Dublin, Ireland.

Jaquire, V., Duvenage, P., & von Solms, S. (2018). 'Building the Ideal Cyber Counterintelligence Dream Team', *17th European Conference on Cyber Warfare and Security*, (pp. 224-232). Oslo, Norway.

Kissel, R., & Wilson, M. (2010). 'Cyber Security Education, Training, and Awareness' in J. G. Voeller (Ed.), Wiley *Handbook of Science and Technology for Homeland Security*, 4 Volume Set. John Wiley & Sons.

MacCauvlei Learning Academy. (2016). *Higher Certificate in Occupational Directed Education, Training and Development Practices*. Pretoria: unpublished.

Monk, T., van Niekerk, J., & von Solms, R. (2010). 'Sweetening the Medicine: Educating Users about Information Security by means of Game Play', *2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists* (pp. 193-200). Bela Bela, South Africa: SAICSIT.

Roper, C., Grau, J., & Fischer, L. (2006). *Security Education, Awareness, and Training: From Theory to Practice*. Oxford: Elsevier Inc.

Thomason, S. (2013). 'People –The Weak Link in Security', *Global Journal of Computer Science and Technology Network*, Web & Security, 13(11).

Toth, P., & Klein, P. (2013, October). *NIST Special Publication 800-16. A Role-Based Model for Federal Information Technology/ Cyber Security Training*. Retrieved September 2018, from http://csrc.nist.gov/publications/PubsDrafts.html#800-16-rev1

Van Derwerken, J., & Ubell, R. (2011). 'Training on the Cyber Security Frontlines' *American Society for Training & Development*, pp 46-50.

.

ANNEXURE K

ECCWS 2019

Coimbra, Portugal

18th European Conference on Cyber Warfare and Security

University of Coimbra

4-5 July 2019

ISBN 978-1-911218-85-2

For further information contact
info@academic-conferences.org
or telephone
+44-(0)-118-972-4148

A Cyber Counterintelligence Matrix for Outsmarting your Adversaries

Petrus Duvenage, Victor Jaquire and Sebastian von Solms
University of Johannesburg, South Africa

duvenage@live.co.za
jaquire@gmail.com
basievs@uj.ac.za

Abstract: While cyber counterintelligence (CCI) has been a distinctive specialisation field for state security structures internationally for well over a decade, there has of late been growing recognition of CCI's significance to also non-state actors. CCI is gaining main stream traction and is seen a central to proactively mitigating cyber risk and exploiting opportunities. The cybersecurity vendor Panda Labs (2018), for example, recently observed that CCI has increasingly become "more significant among larger companies." Also for smaller role-players which do not have resources for a fully-fledged capacity, CCI offers a way of thinking and an approach towards more robustly asserting their cyber interests. With the growing recognition of CCI's significance, comes an acknowledgment of its complexity. CCI is not an easy to use add-on or plug-in. It is all about the meticulous outthinking and outwitting of both actual and potential adversaries. This paper advances a matrix that on practical level can serve as a concise, high-level 'pocket guide' for outsmarting adversaries by means of a robustly configured CCI endeavour. The matrix's uses include (i) guiding the optimal deployment of offensive and defensive tools; (ii) synchronising CCI with broader organisational processes; and (iii) enabling the configuration of a CCI posture most attuned to particular organisations' requirements.

Keywords: Cyber security, cyber counterintelligence, risk management, offensive cybersecurity, threat intelligence.

1. Introduction

The breach of the hospitality giant Marriott International - which made headlines in 2018 and exposed more than 500 million customer records - was the second largest to date (Harvard 2018). The Marriot hack is surpassed only by Yahoo's admission in 2017 that breaches affected around three billion of its user accounts (Harvard 2018). Although attribution is contested, both the Marriott and Yahoo hacks are now widely deemed as the work of nation-state sponsored intelligence actors. These actors are also responsible for numerous other damaging cyber-attacks on non-state actors not previously deemed as the in the cross hairs of state intelligence structures. Concurrently, non-state organisations are also increasingly targeted by also other classes of actors with significant intelligence capacities such as crime syndicated, competitors and some corporate entities (coats 2018). Unsurprisingly, then cyber counterintelligence (CCI) has increasingly become "more significant among larger companies" (Panda 2018). For smaller role-players which do not have resources for a fully-fledged capacity, CCI offers a way of thinking and an approach towards more robustly assert their cyber interests (Jaquire, Duvenage & von Solms 2018). With the growing recognition of CCI's significance, comes an acknowledgment of its complexity. CCI is not an easy to use add-on or plug-in. It is all about the meticulous outthinking and outwitting of both actual and potential adversaries. This paper advances a matrix that can serves as a concise, high-level 'pocket guide' for outsmarting adversaries through a robust CCI endeavour. Premised on CCI's passive-defensive and active-offensive dimensions, the matrix (i) guides the optimal deployment of offensive and defensive tools (iii) synchronises CCI with the organisational processes, (iii) and aids the configuration of a CCI posture best- suited for organisations' varying requirements.

The rest of the paper consists of the following of five parts:

- A cursory overview of the CCI matrix and its two composite parts (namely a vertical plane and a horizontal plane)
- Expounding the CCI matrix's horizontal plane which explains CCI's passive-active and defensive-offensive modes.
- Discussing the CCI matrix's vertical plane by means of which we explicate the different levels of CCI's execution, namely strategic, operational and tactical-technical.
- Presentation of a case study to illustrate the CCI matrix's application.
- Conclusion and observations on future research.

2. Overview of the CCI Matrix

The CCI matrix we advance in this paper comprises a vertical and horizontal plane which can graphically be presented as follow:

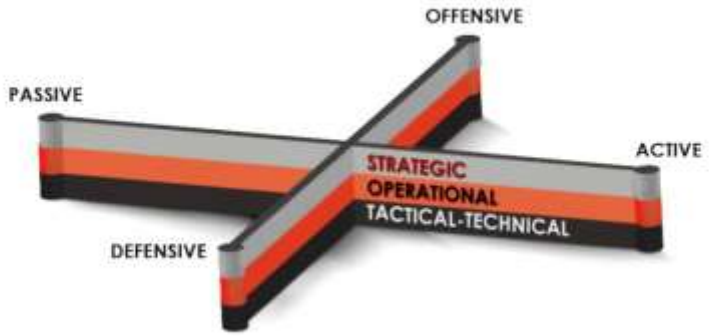


Figure 1: The Cyber Counterintelligence Matrix (Authors)

The CCI matrix's horizontal plane depicted in Figure 1, represents the four quadrants of the CCI postures, namely:

(1) Passive-defensive
(2) Active-defensive
(3) Active-offensive
(4) Passive-offensive

The CCI matrix's vertical plane aligns CCI with broader organisational processes (such as counterintelligence - CI) at the three organisational levels/layers on which CCI operates, namely:

(1) Strategic
(2) Operational
(3) Tactical/Technical

In this section, we briefly outlined the CCI matrix's composition. In the next section, the CCI matrix's vertical plane is discussed.

3. Horizontal Plane of the Matrix: The Cyber Counterintelligence Modes

In the paper's introduction we observed that CCI is a CCI is not an easy to use add-on or plug-in. To be effective, CCI needs to be executed as part an organisation's CI endeavour. As a subset of CI, CCI are underpinned by time-tested CI principles and notions.

3.1 Counterintelligence fundamentals underpinning the CCI matrix

Our CCI matrix's horizontal plane is premised on such two fundamental CI notions. Firstly, that, for a significant part, the wide array of CI measures and tools can be used for defensive and/or offensive purposes. Secondly, that both offensive and defensive tools can be deployed passively and/or actively. Flowing from these two assertions, we can thus infer four modes for deploying CI tools, namely: passive–defensive, active-defensive, passive-offensive and active-offensive. Within CI generally, these modes can be summarised in tabulated format as follows (adapted from Duvenage & von Solms 2014, as compiled from narratives in Prunckun 2012, Sims 2009):

Table 1: Four-sector Counterintelligence Matrix (adapted from Duvenage & von Solms 2014)

DEFENSIVE MODE **Denies adversaries access and gathers intelligence on adversaries**	
Passive Defence Mode Denies the adversary access to information through physical security measures and other security systems.	**Active Defence Mode** The active collection of information on the adversary to determine its sponsor, modus operandi, network and targets. Methods include physical and electronic surveillance, dangles, double agents, moles and electronic tapping.
OFFENSIVE MODE **Primarily aims at exploit, manipulate, degrade and neutralise adversarial intelligence. Also gathers intelligence on adversaries' intelligence activities.**	
Passive Offensive Mode Reveals to the adversary what you want them to see. This could range from selective exposure of actual information to decoys and dummies. The adversary is thus left to draw its own inferences and interpretations.	**Active Offensive Mode** The adversary is fed with disinformation and its interpretation thereof manipulated. Disinformation can be channelled through for example double agents and 'moles'. Active-offensive CI could include some forms of covert action. *

* Covert action, in context of its use in the table, denotes the targeting of an adversary through the influencing of events, conditions, individuals, groups or institutions; to the benefit of a sponsor in a manner not attributable to the sponsor or offering plausible deniability. Influencing is achieved through measures that vary from paramilitary and political actions to propaganda and intelligence assistance.

3.2 Application of the four sector counterintelligence matrix to cyber counterintelligence

The four-sector CI matrix is applicable to the full spectrum of CCI tools. At the one end of the spectrum, conventional intrusion prevention systems (IPS)/intrusion detection systems (IDS) serve as examples of passive–defensive tools. At the other end of the spectrum, a cyber weapon designed to destroy, disrupt or manipulate an opponent's systems constitutes an active-offensive tool. CCI tools can seldom be pigeonholed as having only a defensive or offensive purpose, or as being either active or passive. For the most part, to reiterate, one of the paper's recurring emphases, tools are useful to two or more of the four modes. A honeynet, for example, can be used passive-offensively (e.g. to feed disinformation to an adversary) and active-defensively (e.g. to collect information on an opponent). Graphically, this can be depicted as follows:

Figure 2: Some CCI Tools Plotted on the CCI Matrix's Horizontal Plane (Authors)

As an academic construct, Figure 2 is useful for the categorisation of CCI tools and to explain their relationship with CI tools in fields other than the cyber field. In CCI practice, Figure 2 could have the following three uses:

(1) **Ensure each CCI tool is utilised to maximum effect**. Since most tools can have more than one purpose, they should be measured against the CCI matrix with the question 'In addition to its initially intended role, in what other modes can the tool be used?' Figure2, for example, depicts a honeynet deployed in both the active-defensive and passive-offensive modes. To expand on the example used in Figure2. A honeynet can (if required and depending on circumstances) also be used to facilitate hacking back and the deployment of cyber weapons (active-offensive). If otherwise configured, a honeynet could furthermore be deployed in tandem with IDS/IPS (passive-defensive). In this hypothetical example, a honeynet is therefore relevant to all four modes.

(2) **Synchronise CCI tools/actions with other CI tools/actions**. The plotting of CCI and other CI tools/actions in Figure 2 will aid the synchronisation of efforts and thus optimise the effectiveness and integration of the CI efforts. The feeding of disinformation through a human agent, to use the example depicted in Figure 2 (passive-offensive mode), should be congruent with disinformation 'planted' in an organisation's honeynet. Incongruencies between these two 'feeds' of disinformation could comprise both CI HUMINT and CCI operations. Similarly, the CCI matrix can be utilises to plot and synchronise CCI tools and actions with those in other Technical Intelligence (TECHINT) fields.

(3) **Configure the CCI posture in accordance with the type and needs of a specific organisation**. Statutory military and intelligence services, for example, will typically have a substantial amount of resources directed to the active-offensive mode. The same will not be the case in relation to, for example, a healthcare provider. Figure 2 can accordingly be used as a template for plotting and appropriately configuring an organisation's CCI posture (See for example Jaquire 2018, Appendix6). For purposes of this paper, we suffice with the following (admittedly oversimplified) comparison:

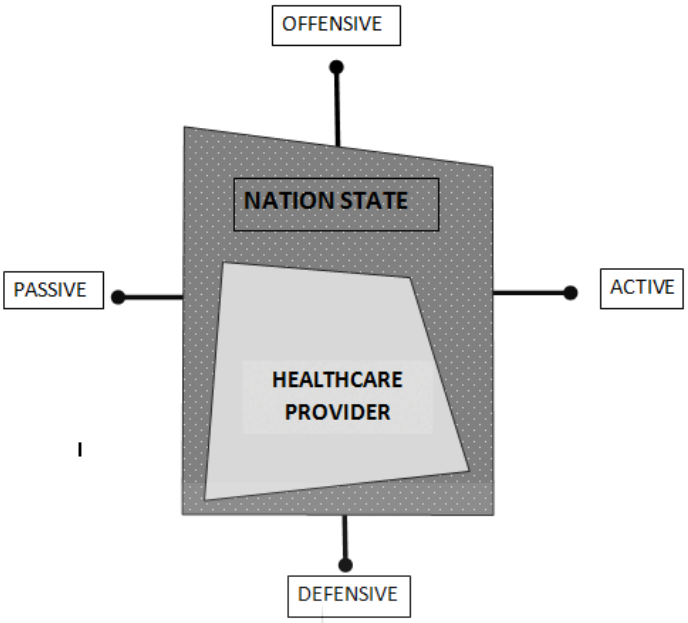


Figure 3: Juxtaposing CCI postures of a nation-state security structure and health care provider (Authors)

Implicit to the comparison per Figure 3 is the notion that the configuration of the organisation's CCI posture on the strategic (interests, goals and strategy) levels will ultimately shape CCI activities on the operational and tactical-technical level. These different levels are discussed in the next section as the CC matrix's horizontal plane.

4. Vertical Plane of the CCI Matrix: Levels of Execution

The CCI matrix's vertical plane explains the various levels on which CCI functions and integrates CCI with the broader organisational postures and processes. Since CCI is a CI subset, the importance of synchronising and integrating CCI with especially the organisational CI endeavour on all levels can hardly be overemphasised. As was the case with the development of the horizontal plane, we based our design of the vertical plane on an established CI notion, namely the three levels/layers of execution (strategic, operational and tactical). These levels and there interplay have been described in more detail in existing research (van Niekerk & Duvenage 2016; Duvenage, Jaquire & von Solms 2016; Stech & Heckman 2018, Jaquire 2018). Therefore, this paper suffices with the following synopsis:

Table 2*:* Synopsis of the Levels of CCI Execution (adapted from Duvenage, Jaquire & von Solms 2016)

Table 2 follows on the next page

	Strategic	Operational	Tactical/Technical
CI mission	• Advance and protect organisational interests through defence against and the offensive engagement of adversarial intelligence activities. This is achieved through the following functions: detect, deny, deter, deceive, degrade and/or disrupt.		
CCI mission	• As above, when the adversary uses cyber as a conduit or a cyber asset as a target.		
Leadership	• C-level	• Senior and middle management	• Line and team leaders
Interface with CI	• Organisational, intelligence and CI strategies • All-source CI feed	• Multidisciplinary programmes and operations	• Multidisciplinary projects and continuous line-functional interaction
Referent objects	• Organisation's 'crown jewels' • Critical information and cyber-assets sought (e.g. adversary's 'crown jewels') • Conditions (competitive advantage)	• People, processes, systems, procedures (personal security, ICT architecture and supply-chain management) • Own intelligence programme	• Systems, networks and devices • Network operations • Security operations • CIA (confidentiality, integrity and availability)
Interrogatives	• Who, why?	• Who, where, when, how?	• What, how?
Level ofadversarial role-player (CCI focus)	• Sponsors, opponents and Intelligence capacity	• Intelligence structures, groups and campaigns	• Individuals, TTPs, incidents and actions (on-the-network)
Indicators of targeting and compromise	• Geo-political, sector/industry 'flags' • Analogous events • Adversarial strategy and business decisions	• Operational disruption • Organisational and/or revenue decline • Information leakage	• Breach in the C-I-A of cyber and/or information security milieu • Identification of malicious code, intrusion and threat exploitation
Analysis output	• High-level, strategic appraisals • Strategic warning and advisories	• Operational reports (CCI operations, threat, damage and vulnerability assessments, alerts and warnings) • Trend analyses	• Tactical and technical information reports • Alerts and warnings
Tools – means, methods and measures (offensive, defensive & collection)	• Multidiscipline CI • Strategic direction of means, methods and measures	• For a **taxonomy of the wide array of CCI** tools see (Duvenage, Jaquire& von Solms 2016; Jaquire 2018). • Interlocked with operational and tactical CI	
Cyber threat intelligence (sourced)	• White papers, non-commissioned and non-commissioned research	• Platforms	• Data feeds
Skill sets required (line-functional)	• Sound knowledge of business and industry • Specialised knowledge and skills in intelligence, multidisciplinary CI and CCI • Strategic analysis and management	• Multi-disciplinary CI • CCI operational and/or technical specialisation • Operational management • Elements of both strategic and tactical	• ICT and information security • Systems, software development, scripting and programming • CCI and CCI technical specialisation • Ethical hacking • Technical cyber defence and collection • Humanities, social sciences and languages • HUMINT • Engineering and reverse engineering

In this section we CCI levels of execution as the CCI matrix's vertical plane. We now proceed with illustrating the matrix's application by means of Stech and Heckman's (2018) hypothetical case study.

3.3 The CCI matrix in practice – a hypothetical case study

As was observed in Section 3.2, the organisation's CCI posture on the strategic (interests, goals and strategy) level will shape CCI activities on the operational and tactical-technical levels. It then logically follows that strategy and operational objectives will determine the offensive-defensive, passive-active modes on a tactical-

technical level. This point, as well as the application of our CCI matrix, are illustrated by Stech and Heckman's (2018) proposition on a "Cyber Counterintelligence Framework in Active Defense". Utilising a hypothetical case study of a NATO campaign against "advanced persistent threat actors associated with Russia, APT28 and APT28", Stech and Heckman (2018) pose the following as NATO's strategic CCI goal and operational objectives:

- "Support NATO strategic deception goal: convince Russian authorities their cyber intelligence supports propaganda but is not ready for kinetic war against NATO;
- Active & Passive CCI Defense: Reduce and eliminate effectiveness of APT28 tactics, techniques, and procedures for espionage; Eliminate or counter APT28 and APT29 malware and tradecraft;
- Passive CCI Offense: Poison APT28 and APT29 intelligence stream with deception materials; eliminate, corrupt, or covertly take over control of attackers' command and control; and
- Active CCI Offense: Feed Russian espionage units with false information (e.g. feed APT29 false information about actions and effects of APT28, and *vice versa*).
- Support apparent intrusion successes with cyber and non-cyber strategic NATO deception operations."

In extending the strategic goal and operational objectives to the tactical-technical level, Stech and Heckman (2018) apply our four-sector matrix (advanced per Duvenage & von Solms 2013 and further developed in Table 2 of this paper) advanced earlier in this paper) – as follows:

Table 3: Hypothetical NATO Cyber CI Operations against cyber espionage threat (Stech & Heckman 2018)

Modes	Passive Cyber CI	Active Cyber CI
Defensive mode	**Deny access and collect on espionage threat**	
	Passive defense:	**Active defense:**
	Harden endpoint and server configurations	Gather intelligence on on-going intrusions
		Use honeypots to gather late-stage implants and unpatched exploits
	Share actionable indicators across NATO intelligence partners	
		Share indicators to force infrastructure and "toolkit" rotations
Offensive Mode	**Manipulate, degrade, control and neutralize espionage threat**	
	Passive offensive:	**Active offensive:**
	Use honeypots to deliver deception materials	Counter-hack hop points and control servers
		Trolling "bait victims" to lure attackers to controlled boxes
	Sinkhole APT28 hop points	
	Identify APT28 operatives	Operating controlled boxes as double agents to inject beacons, double-hacked backdoors, etc. into APT28 control environment

In this section, we illustrated the application of our four-mode, three-tiered matrix by citing Stech& Heckman's (2018) hypothetical NATO case study. We now proceed with observations in conclusion.

5. Conclusion

This paper is submitted within the context of non-state entities' growing adoption of CCI in the face of escalating targeting by intelligence actors of various categories. CCI undoubtedly offers a practicable approach to protect and advance organisational interests. There is, however, a precondition and qualification. CCI not meticulously configured, is more likely to be self-defeating than beneficial. Moving from this premise, key findings of this paper include the following:

- A CCI matrix can aid the configuration of a robust cybersecurity posture and the exploitation of opportunities.
- Such a CCI matrix can be constructed by combining (i) CCI's Passive-Active and Defensive-Offensive modes; and (ii) CCI's levels of execution namely: Strategic, Operational and Tactical-Technical.

On an academic level, the CCI matrix could be useful to conceptually structure aspects of research in this fast growing field.

References

Coats, D.R. (2018) *Worldwide threat assessment of the US Intelligence Community February 13, 2018,* accessed on 27/07/2018 at https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2016) 'Conceptualising cyber counterintelligence – Two tentative building blocks' in *Published Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, Germany, June.

Duvenage, P., & von Solms, S. (2013). 'The Case for Cyber Counterintelligence', *International Conference on Adaptive Science and Technology*. Pretoria, South Africa: IEEE.

Duvenage, P.C. & von Solms, S.H. (2014) 'Putting counterintelligence in cyber counterintelligence' in *Published Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece, July.

Duvenage, P., & von Solms, S. (2015). 'Cyber Counterintelligence: Back to the Future', *Journal of Information Warfare*, 13(4), 42-56.

Harvard University (2018): *Certificate -Managing Risk in the Information Age*, course material, Office of the Vice Provost for Learning Advances (VPAL), Massachusetts, US.

Jaquire, V.J. (2018) *A framework for a cyber counterintelligence maturity model*, D.Com (Informatics) thesis, University of Johannesburg, Johannesburg, South Africa.

Jaquire, V.J., Duvenage, P.C. & von Solms, S.H. (2018) ' Building the CCI dream team' in *Published Proceedings of the 17th European Conference on Cyber Warfare and Security*, Oslo, Norway, June.

Panda Security (2018) *The hunter becomes the hunted: How cyber counterintelligence works*, accessed on 06/11.2018at https://www.pandasecurity.com/mediacenter/panda-security/cyber-counterintelligence/

Prunckun, H. (2012) *Counterintelligence: Theory and practice*, Rowman & Littlefield Publishers, Plymouth, UK.

Stech F.J. & Heckman K.E. (2018) 'Human Nature and Cyber Weaponry: Use of Denial and Deception in Cyber Counterintelligence' in Prunckun, H (ed.) *Cyber Weaponry Issues and Implications of Digital Arms*, Springer, Cham, Switzerland.

Sims, J.E. (2009) 'Twenty-first-century counterintelligence' in Sims, J.E. &Gerber, B. (eds) *Vaults, mirrors and masks – Rediscovering U.S. counterintelligence,* Georgetown University Press, Washington D.C., US.

van Niekerk, B. & Duvenage, P. and (2016). "Cyber Intelligence and Counterintelligence,"*ISACA South Africa Conference 2016*, Johannesburg, 29-30 August.

ANNEXURE L

ECCWS 2019

Coimbra, Portugal

18th European Conference on Cyber Warfare and Security

University of Coimbra

4-5 July 2019

ISBN 978-1-911218-85-2

For further information contact

info@academic-conferences.org

or telephone

+44-(0)-118-972-4148

An Analysis of Selected Cyber Intelligence Texts

Brett van Niekerk[1], Trishana Ramluckan[1], and Petrus Duvenage[2]
[1]University of KwaZulu-Natal, Durban, South Africa
[2]University of Johannesburg, Johannesburg, South Africa

vanniekerkb@ukzn.ac.za
ramluckant@ukzn.ac.za
duvenage@live.co.za

Abstract: Cyber intelligence is a growing discipline related to cyber security, resulting in a number of whitepapers, advisories and services from cyber security companies and professional bodies. Global spending on cyber threat intelligence services has demonstrated rapid increases, yet a corresponding mitigation of advanced threats is yet to be seen. Despite this growth, there is still variation on the definition and the focus of cyber intelligence, which could account for the limited gains. Cyber intelligence is important for understanding both the threat environment and identifying what is relevant to the user's context based on a number of internal factors to the organisation or nation. This paper provides a document analysis of a number of publicly available cyber intelligence and cyber threat intelligence documents (in the form of advisories and whitepapers) using text mining, content analysis, and thematic analysis. These techniques are relevant to both qualitative research and intelligence analysis and are employed here for assessing similarities amongst the documents, identifying common themes and categories, assessing the emphasis thereof, and identifying gaps common to these documents. Gaps in the coverage of the documents are identified in that they do not consider cyber counterintelligence or the legal considerations for cyber intelligence, and cyber intelligence collection operations are only briefly mentioned. Cyber counterintelligence and cyber intelligence collection operations are sub-disciplines of cyber intelligence, alongside cyber threat intelligence. The analysis also indicates that documents on cyber intelligence and cyber threat intelligence do not align. Such occurrences and some implications thereof are discussed.

Keywords: Qualitative analysis, Cyber Intelligence, Cyber Counterintelligence, Cyber Law

1. Introduction

The 2019 US National Intelligence Strategy is placing emphasis on cyber security (Office of the Director of National Intelligence, 2019); by extension this implies increasing focus on cyber intelligence. Cyber threat intelligence services have seen a great deal of attention and an increase in subscriptions, with a growth of 129% in four years (Duvenage & van Niekerk, 2016), however this has not yet translated into widespread effective mitigation of cyber threats. Despite the increase in the prevalence of cyber threat intelligence, there is still uncertainty surrounding the definitions and the focus of cyber intelligence. This uncertainty can negatively affect the understanding of the topic and ultimately the effectiveness of implementations, which could account for the limited gains.

It is worthwhile to provide the definition of intelligence, as this useful to distinguish amongst various concepts covered in this paper. Intelligence is a product of the collection, processing, analysis, and interpretation of information about nations, actors, threats, and operational areas (Joint Chiefs of Staff, 2013); it needs to be in context and actionable. There is a difference between cyber intelligence and cyber espionage: cyber intelligence seeks to gain information and insights about relevant cyber threats, whereas cyber espionage is the use of cyber techniques to steal secrets (Duvenage & van Niekerk, 2016).

Lee (2014a; 2014b) considers cyber intelligence to be comprised of the following sub-disciplines: cyber threat intelligence (CTI) (Lee, 2014e), cyber intelligence collection operations (Lee, 2014c) and cyber counterintelligence (CCI) (Lee, 2014d). CTI can be seen as subscription services providing information input for intelligence analysis, whereas collection operations can be considered as obtaining specific external and internal information for analysis. Counterintelligence is both provocative and defensive intelligence operations: mitigating adversary collection operations whilst seeking to learn more regarding their objectives and techniques (Lee, 2014b; 2014d). These components are depicted in Figure 1.

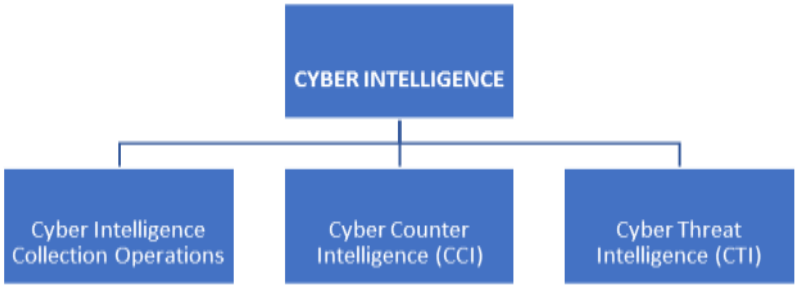


Figure 1: Components of Cyber Intelligence

Both intelligence and cyber security are multi-disciplinary topics. Cyber security traditionally will contain the technical subjects; however, the strategic political and legal aspects are coming to the fore. Similarly, intelligence studies have a traditional focus on politics and history, but there is a growing situation where other disciplines can contribute to intelligence studies (Marrin & Madison, 2017); particularly with the growth of computing and cyber security. In the same manner, academic research methodology can be useful in intelligence analysis for cyber security.

The Introduction continues below in Section 1.1. where an overview of related research and publications are provided. Section 2 presents the methodology, introducing the documents and the techniques used to assess them. Section 3 provides the results of the analysis of the texts, which is followed by a discussion of the results in Section 4. A discussion on the techniques used in this study and their multi-disciplinary use for cyber intelligence analysis is provided in Section 5. The paper is concluded in Section 6.

1.1 Related Research and Publications

A number of previous research outputs have considered cyber intelligence from different perspectives. One of the first works considering cyber intelligence was by Bodmer, Kilger, Carpenter, and Jones (2012), which focussed on counter intelligence principles for network security. Yucel Koltuksuz (2014) provide a list of articles for topics such as cyber espionage, open source intelligence, social media intelligence, threat and intrusion detection, and cyber weapons. Falk (2016) proposes an initial ontology describing aspects related to CTI. Sample, Cowley, Watson, and Maple (2016) investigate the possibility of cultural influences in CTI, and found possible links between national culture and activities of the threats, which could conceivably be used for attribution or deception. Duvenage, Jaquire, and von Solms (2016) consider the relationship between CCI and CTI, and categorise offensive and defensive CCI. Bellaby (2016) motivates for cyber intelligence whilst warning against misuses, and considers some legal aspects to guide conducting cyber intelligence operations. One of the gaps that has not been assessed are the cyber intelligence documents produced by professional bodies to guide organisations and cyber security professionals. This paper analyses eight selected texts from three professional bodies. The next section describes the texts and analysis techniques in more detail.

2. Methodology

Qualitative analysis of cyber intelligence whitepapers and best practices is conducted, in particular content analysis and thematic analysis of the documents. In total eight documents were selected from professional bodies based on their relationship with the topic. These texts include: ISACA Tech Brief on Threat Intelligence (2017), Centre for the Protection of National Infrastructure Threat Intelligence whitepapers by Context (2015) and MWR InfoSec (2015), and Intelligence and National Security Alliance (INSA) documents as listed below:

- Cyber Intelligence – Setting the Landscape for an Emerging Discipline (INSA, 2011);
- Operational Levels of Cyber Intelligence (INSA, 2013);
- Strategic Cyber Intelligence (INSA, 2014a);
- Operational Cyber Intelligence (INSA, 2014b);
- Tactical Cyber Intelligence (INSA, 2015).

The software NVivo was used to conduct the analysis – this provides content analysis in terms of the frequency of major words in the texts. Thematic analysis provides an indication of the prevalent themes in the texts.

Document correlation and cluster analysis is also performed. This indicates relationships amongst the various themes and documents.

3. Analysis of Cyber Intelligence White Papers

Figure 2 provides a cluster analysis of the documents based on word similarity, determined using Pearson's correlation. There are two main clusters: the documents focussing on threat intelligence, and the INSA documents focussing on the operational levels of cyber intelligence. From the cluster, it can be seen that the document on tactical cyber intelligence is closest to the threat intelligence documents, followed by operational and then strategic. This indicates that the focus on the threat intelligence is tactical in nature, aligning more to the cyber-security analysts rather than aiding organisational or national decision makers in defining cyber-security strategies.

Figure 2: Sources Clustered based on Word Similarity

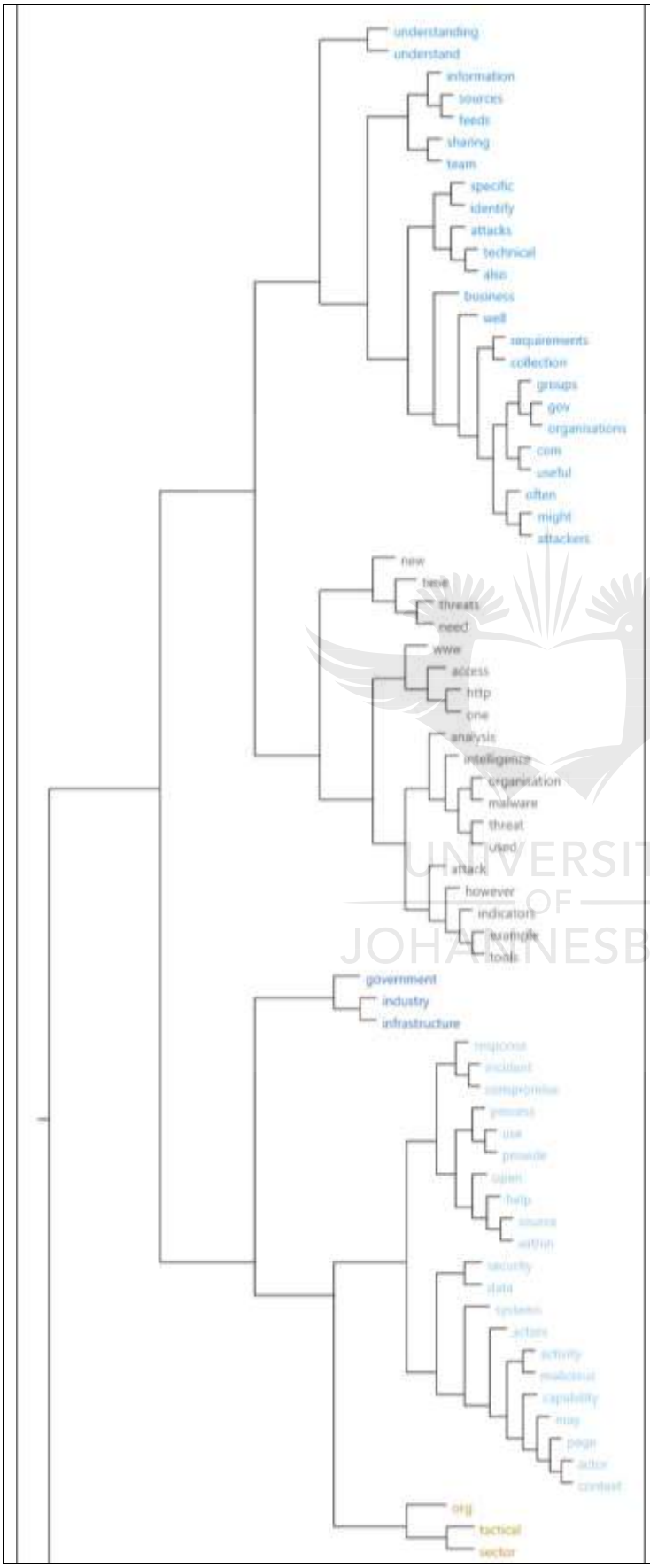
The overall word frequency is visualised in Figure 3. The larger the word, the more common. Despite there being more documents in cyber intelligence operational levels (five of the eight), the word 'cyber' is not as prevalent as the word 'threat'. The words following this in prevalence are: 'information', 'security', 'organisation' and 'network'.

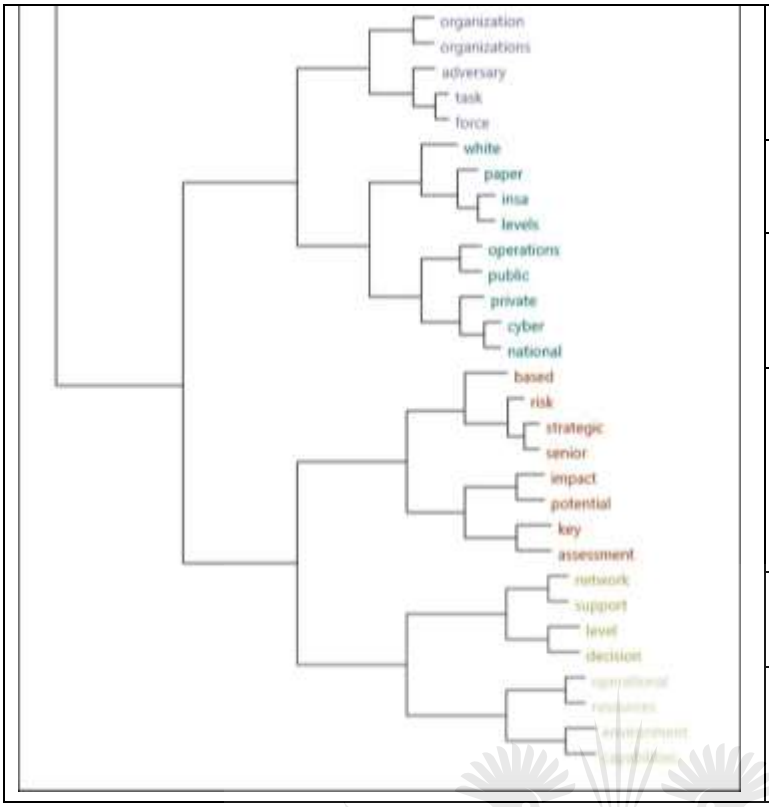
Figure 3: Word Cloud from all Texts

The content analysis determines the frequency of words. Figure 4 clusters these words to determine key themes across the texts (indicated on the right). Key themes that emerge are: collection and sharing of information; technical intelligence; business requirements; actors; new threats; intelligence analysis; attacker tactics, techniques and procedures (TTPs); targets; incident response; system security data; Actors activities and capabilities; tactical aspects in organisations sectors; national cyber consideration e.g. public vs private; strategic intelligence and risk; decision making levels; and operational considerations.

From the clustering of the words, it is implied that threat intelligence is tactical and focussed at the organisational level, whereas strategic cyber intelligence is more related to a national focus. Aspects that are noticeably absent from the word cloud and word cluster analysis are the concept of cyber intelligence

collection operations, cyber counterintelligence, and any legal or governance aspects related to cyber intelligence. The linkages of analysis techniques to the usage of intelligence is also not covered in detail.

	
	Collection and sharing of information
	Technical intelligence – specific identification of attacks
	Business / collection requirements
	Actors / Attackers – groups/governments/organisation
	New threats
	Analysis of intelligence – threats & malware
	Attacker TTPs: IOC
	Targets
	Incident response
	System security data
	Actors activities and capabilities
	Tactical: organisation & sector



National cyber; public & private
Strategic intelligence: risk information
Levels of decision making and network support
Operational considerations: resources, environments, capabilities

Figure 4: Cluster Analysis of Key Words

4. Discussion of Results

The discussion is divided into two section: the first (Section 4.1) provides a discussion on the explicit content analysis. The second (Section 4.2) provides a discussion on the gaps of content coverage that are indicated above.

4.1 Discussion of Document Analysis

The two distinct clusters in the document correlation implies that threat intelligence and cyber intelligence are not the same; and that there is some misalignment between those considering cyber intelligence holistically and those considering threat intelligence. The tactical cyber intelligence appears closest to the threat intelligence, indicating that the focus of the threat intelligence is towards detection of possible indicators at an analyst level, and there is limited threat intelligence to aid strategic decision makers. This view concurs with that of Lee (2014e).

There appears to be a focus on CTI. As Lee(2014b) and Duvenage, Jaquire, and von Solms (2016) indicated, the focus on CTI is more due to a catch-phrase in marketing services than real understanding of the concepts. CTI as is provided cannot be considered true intelligence as it is a stream of data; it is not in context and it is limited in how actionable it is. Whilst network security devices and cyber security analysts can use CTI as an aid in detecting possible threats, the real intelligence is the analysis and interpretation of any indicators that have found matches in the network. Therefore, CTI on its own is of limited use; it needs to correlated with internal data (processing) to provide possible threat detections, which can then be analysed and interpreted to form an improved view of the threat environment.

4.2 Gaps in Document Coverage

As is indicated in Section 3, there are gaps in the coverage of the documents. This includes the concept of cyber intelligence collection operations and cyber counterintelligence (Section 4.2.1), legal and governance considerations (Section 4.2.2), and the linkage of analysis techniques and usage (Section 4.2.3).

4.2.1 Cyber Intelligence Collection Operations and Cyber Counterintelligence (CCI)

None of the documents consider cyber counterintelligence, and cyber intelligence collection is only briefly considered at a high level. As is evident from Figure 3, the term "collection" does not occur frequently. These are key constructs in cyber intelligence, and the limited coverage illustrates the gaps in professional literature.

Intelligence collection is considered at a high level, however specific techniques for collection are not covered in detail. Certain sources may be best suited for a specific level of intelligence (tactical/technical, operational, or strategic), and the collection methods for those sources may differ. The INSA (2014b) document provides the most detail for the collection processes and considerations. As CTI is essentially a data stream with a very broad context, collection operations are important to gain insights into the internal environment against which the CTI can be correlated. This is known as passive collection (Lee, 2014c). Active collection is the process of obtaining intelligence off of an adversary's network (Lee, 2014c). This activity is considered unethical or illegal for non-state actors to conduct, as is outlined by the Singapore Norm Package by the Global Commission on the Stability of Cyberspace (GCSS, 2018), which will be discussed in more detail in Section 4.2.2.

It is also important to note that the network environment can influence the choice of collection techniques. For instance, industrial control networks are particularly sensitive, therefore collection operations from critical infrastructures may have unintended adverse impacts resulting in downtime of the control systems. The increase of connected 'smart' devices (Internet of Things) through the Fourth Industrial Revolution can provide challenges. These devices can increase the attack surface, and due to the quantity of the devices, there may be an overload of information, which may result in additional pre-processing to filter out. As many devices can connect in an ad-hoc or uncontrolled manner, they may be invisible to collection operations if they are not connected during the period of the collection. Therefore, insecure devices could be missed, giving an inaccurate picture of the threat exposure.

Cyber counterintelligence is an important concept as this can be seen as defending against adversary network intrusions and espionage or intelligence collection operations, whilst obtaining critical information regarding their tactics, techniques, procedures and objectives. Offensive CCI interacts with the adversary (Lee, 2014d) in order to gain an understanding of their objectives and preferred methods. This involves the use of deception such as fake online profiles to engage with the adversary, or the use of honeypots and honeynets to monitor their activity (Bodmer, Kilger, Carpenter, & Jones, 2012). The use of deception has been debated from legal and ethical viewpoints and will be discussed further in Section 4.2.2. Defensive CCI can use red teams and threat analysis techniques to identify specific areas for cyber security improvement specifically based on an organisation's threat and vulnerability landscape (Lee, 2014d). During the past four years it was especially cyber intelligence's component of cyber counterintelligence that has been gaining traction in main stream business (The Economist, 2015; Panda Security, 2018). The growing commercial prominence of cyber intelligence and its subsets raises the academic imperative to clearly delineate concepts within this emerging (academic) field.

4.2.2 Legal and Governance Considerations

With reference to Bodmer, Kilger, Carpenter, & Jones (2012,108), every country or organisation has the capabilities in terms of rules or governance to restrict counterintelligence activities, preventing it from invading the rights of its private citizens. However, in some countries, absolute power belongs to the State, under the pretence of representing freedom and liberty for all its citizens. Therefore, prudence is warranted as counterintelligence professionals conduct their operations. Cyberspace poses a particular challenge as online activities, spread at rapid pace from country to country, with the ability to gather information.

Bodmer, Kilger, Carpenter, & Jones (2012,410), further state that since this many be the case, a number of national and international cyber laws have been developed and are applicable in various countries. The implications of which need to be understood, regardless of the country an individual may reside in or who is hosting the IP address. While some countries may choose to remain unaffected or indifferent, countries like the US, intend prosecuting those individuals (Bodmer, Kilger, Carpenter, & Jones, 2012: 410).

The South African King IV Report Section 13d provisions for the "proactive monitoring of intelligence to identify and respond to incidents." This includes any adverse social media activities as well as cyber-attacks (Institute of Directors Southern Africa (IoDSA), 2016)

The Global Commission on the Stability of Cyberspace 2018's Singapore Norm Package states that "Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur." With reference to Nijman (2010), non-state actors do not have a legal personality, which creates the challenge concerning the legality of intelligence collection from adversary networks by non-state actors. This creates a legal challenge when a government entity attempts to utilise the services of non-state actors as part of their intelligence operations. Since non-state actors have no legal personality within the context of International Law, the question of attribution of liability may arise. With reference to the United Nations (UN) Convention on the Law of the Sea (LOSC), companies may enter into an international contract regarding various services, but in so doing they also incur obligations and responsibility under international law. While the Convention may apply to some shared responsibility between states and international organisations, it can be argued that non-state actors, on the basis of the "contract", would be responsible for wrongful acts and thereby be in breach of the contract. This, however, still falls outside the ambit of International Law, and may just be attributable in terms of a "contractual obligation" (d'Aspremont, Nollkaemper, Plakokefalos and Ryngaert, 2015).

The next consideration is the legality of using "honeypots" for the purpose of counter intelligence. According to Spitzner (2003) there are three main issues that are commonly maintained regarding honeypots which are entrapment, privacy, and liability. By definition entrapment is "a law-enforcement officers or government agent's inducement of a person to commit a crime, by means of fraud or undue persuasion, in an attempt to later bring a criminal prosecution against that person" (Black's Law Dictionary, 7th Ed). From the definition, honeypots do not qualify as a form of entrapment, as the "attacker", usually breaks into a honeypot on their own initiative and coercion is not involved. Regarding privacy, the use of honeypots does affect privacy. The exemption under Service Provider Protection means that security technologies can gather information on people including attackers, as long as that particular technology is being used for the protection of the environment, which results in these technologies are exempt from privacy restrictions (Spitzner, 2003). Spitzner (2003) states that liability implies a person can be sued if their honeypot is used to harm others, however, it is a civil matter and not a criminal one.

There remains the need for cyber intelligence governance as cyber intelligence needs to cooperate with legal counsel pertaining to the issues (Bodmer, Kilger, Carpenter, & Jones, 2012: 169).

4.2.3 Analysis Techniques and Usage

Depending on the sector or organisation type, the use of cyber intelligence, and therefore the analysis techniques, may differ. The intelligence required for a private organisation will be different to that of a nation state, where the military, intelligence community, and law enforcement are producers and consumers of cyber intelligence. Non-state organisations are more likely to be intelligence consumers, where the processing may be limited to distilling the intelligence further to make it more relevant to the organisation's context. The various organs of state mentioned above will be required to provide collection, processing, analysis and interpretation within their mandates to achieve their objectives; they are therefore both producers and consumers of cyber intelligence.

As with the cyber intelligence collection operations, the INSA (2014b) document has the most detail of potential analysis techniques for cyber intelligence. The analysis techniques need to be carefully selected, as they need to be relevant to the data types and the objectives of the intelligence product. As an example, Heuer and Pherson (2015) describe seven structured analytical techniques to achieve twelve objectives in analysis. Specific cases of employing these techniques are illustrated in Beebe and Pherson (2015). As an extension to this, Section 5 discusses the research methodology used in this paper as a relevant intelligence analysis technique.

5. Research Methodologies and Intelligence Analysis Techniques

This section reflects on research methodology used in this paper and its relevance to cyber intelligence analysis. The research process is very similar to that of intelligence analysis: a problem or question is identified, data is collected, process, and analysed to provide interpretations that are then compiled into an output (a dissertation, paper, or intelligence report).

The qualitative analysis using tools such as Nvivo can quickly provide insights into large bodies of text which will be very time consuming for human analysts to process and assess. Data sources could be official documents (as is used in this paper), or forum discussions on social media or the dark web, or transcripts from speeches. A specific use case could be the assessment of foreign cyber security strategies. By clustering the documents, an analyst could gain an insight into possible influence and/or collaboration amongst nations. This could also simplify analysis of a national cyber security posture as similar nations can be identifies and experience from previous analyses can be leveraged.

On its own, this analysis will not be sufficient. There still needs to be interpretation of the results, where bias in the analysis can still occur. As Heuer and Pherson (2015), critical analysis has led to major intelligence mistakes; therefore, this technique needs to be followed by other analytics techniques to validate the interpretation. This concern is common both the academic research and intelligence analysis. Therefore, the structured analytic techniques advocated by intelligence analysts may prove to be very beneficial in academic research.

6. Conclusion

Cyber intelligence is a rapidly growing field; however, it still suffers from being poorly defined. This paper analysed selected texts from professional bodies. The results indicate that there is a possible misalignment between the drive for cyber threat intelligence and the growth of cyber intelligence as a discipline. Aspects that were found to be omitted are cyber counterintelligence and the legal and governance aspects, with more focus on cyber intelligence collection operations and analysis techniques required. For cyber intelligence to mature as a discipline, the inclusion of these areas, and aligning all areas is imperative. Due to the increasing prevalence in industry, there is a need to ensure that academic studies in these areas grow. The qualitative research methods employed in this paper may prove to be useful in cyber intelligence analysis, and intelligence analysis techniques can be used to improve academic research.

References

Beebe, S.M., and Pherson, R.H. (2015) *Cases in Intelligence Analysis: Structured Analytic Techniques in Action*, 2nd ed., Los Angeles: Sage.

Bellaby, R.W. (2016) "Justifying Cyber-intelligence?" *Journal of Military Ethics*, 15(4), pp. 299-319.

Bodmer, S., Kilger, M., Carpenter, G., and Jones, J. (2012) *Reverse Deception: Organised Cyber Threat Counter-Exploitation*, New York: McGraw-Hill.

d'Aspremont, J., Nollkaemper, A., Plakokefalos, I and Ryngaert, C. (2015). Sharing Responsibility Between Non-State Actors and States in International Law: Introduction. Netherlands International Law Review, Volume 62, Issue 1, pp 49–67.

Duvenage, P. Jaquire, V. & von Solms, S. (2016) "Conceptualising Cyber Counterintelligence: Two Tentative Building Blocks," *Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, 7-8 July, pp. 93-103.

Duvenage, P. and van Niekerk, B. (2016). "Cyber Intelligence and Counterintelligence," *ISACA South Africa Conference 2016*, Johannesburg, 29-30 August.

The Economist. (2015) Manage like a spymaster: Counter-intelligence Techniques may Help Firms Protect Themselves Against Cyber-attacks, 27 August, [online], accessed 24 May 2016, https://www.economist.com/business/2015/08/27/manage-like-a-spymaster.

Falk, C. (2016) "An Ontology for Threat Intelligence," *Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, 7-8 July, pp. 111-116.

ISACA. (2017) *Tech Brief: Threat Intelligence*, [online], accessed 16 November 2017, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Threat-Intelligence.aspx.

Context. (2015) *Integrating Threat Intelligence: Defining an Intelligence Driven Cyber Security Strategy*, Centre for the Protection of National Infrastructure, [online], accessed 12 April 2016, https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/CPNI_CONTEXT_CERT-Threat_Intelligence.pdf.

Garner, BA. (1999). Black's Law Dictionary. 7th Edition. United States of America.

Global Commission on the Stability of Cyberspace. (2018) *Norm Package Singapore*, November, [online], accessed 30 January 2019, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

Heuer, R.J., and Pherson, R.H. (2015) *Structured Analytic Techniques for Intelligence Analysis*, Los Angeles: Sage.

Institute of Directors Southern Africa. (2016) *King IV: Report on Corporate Governance for South Africa 2016*, [online], accessed 28 January 2019, https://www.iodsa.co.za/page/KingIV.

Intelligence and National Security Alliance. (2011) *Cyber Intelligence – Setting the Landscape for an Emerging Discipline*, September, [online], accessed 7 March 2016, https://www.insaonline.org/cyber-intelligence-setting-the-landscape-for-an-emerging-discipline/.

Intelligence and National Security Alliance. (2013) *Operational Levels of Cyber Intelligence*, September, [online], accessed 7 March 2016, https://www.insaonline.org/operational-levels-of-cyber-intelligence/.

Intelligence and National Security Alliance. (2014a) *Strategic Cyber Intelligence*, March, [online], accessed 7 March 2016, https://www.insaonline.org/strategic-cyber-intelligence/.

Intelligence and National Security Alliance. (2014b) *Operational Cyber Intelligence*, October, [online], accessed 7 March 2016, https://www.insaonline.org/operational-cyber-intelligence/.

Intelligence and National Security Alliance. (2015) *Tactical Cyber Intelligence*, December, [online], accessed 7 March 2016, https://www.insaonline.org/tactical-cyber-intelligence/.

Joint Chiefs of Staff. (2013). Joint Intelligence, Joint Publication 2-0,

Lee, R.M. (2014a) "An Introduction to Cyber Intelligence," *Tripwire Blog*, 16 January, [online], accessed 15 March 2018, https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/.

Lee, R.M. (2014b) "Developing Your Cyber Intelligence Analyst Skills," *Tripwire Blog*, 27 January, [online], accessed 15 March 2018, https://www.tripwire.com/state-of-security/security-data-protection/developing-cyber-intelligence-analyst-skills/.

Lee, R.M. (2014c) "Cyber Intelligence Collection Operations," *Tripwire Blog*, 25 February, [online], accessed 15 March 2018, https://www.tripwire.com/state-of-security/security-data-protection/cyber-intelligence-collection-operations/.

Lee, R.M. (2014d) "Cyber Counterintelligence: From Theory to Practice," *Tripwire Blog*, 5 May, [online], accessed 15 March 2018, https://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/.

Lee, R.M. (2014e) "Cyber Threat Intelligence," *Tripwire Blog*, 2 October, [online], accessed 15 March 2018, https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/.

Marrin, S., and Madison, J. (2017) *Intelligence Studies, Intelligence Analysis, and Multidisciplinary Learning*, The National Academies of Sciences, Engineering, Medicine, [online], ccessed 28 January 2019, http://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179893.pdf.

MWR InfoSecurity. (2015) *Threat Intelligence: Collecting, Analysing, Evaluating*, Centre for the Protection of National Infrastructure, [online], accessed 12 April 2016, https://www.ncsc.gov.uk/content/.../MWR_Threat_Intelligence_whitepaper-2015.pdf.

Nijman, J. E. (2010). Non-State Actors and the International Rule of Law: Revisiting the "Realist Theory" of International Legal Personality, Non-State Actors in International Law, Politics and Governance Series. 5.

Office of the Director of National Intelligence. (2019). *National Intelligence Strategy of the United States of America 2019*, [online], accessed 28 January 2019, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

Panda Security (2018) *The hunter becomes the hunted: How cyber counterintelligence works*, 6 July, [online], accessed on 06 November 2018, https://www.pandasecurity.com/mediacenter/panda-security/cyber-counterintelligence/.

Sample, C., Cowley, J., Watson, T., and Maple, C. (2016) "Re-thinking Threat Intelligence," *International Conference on Cyber Conflict* (CyCon U.S.), Washington, DC, USA, pp. 1-9.

Spitzner, L. (2003). Honeypots: Are They Illegal? Symantec [online], accessed 8 February 2019, https://www.symantec.com/connect/articles/honeypots-are-they-illegal

Yucel, C., and Koltuksuz, A. (2014) "An Annotated Bibliographical Survey on Cyber Intelligence for Cyber Intelligence Officers," *Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece, 3-4 July, pp. 213-220.